Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Army Network-Enabled Operations: Expectations, Performance, and Opportunities for Future Improvements	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **RAND Corporation,Arroyo Center,1776 Main Street, P.O. Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**245**	

This product is part of the RAND Corporation monograph series. RAND monographs present major research findings that address the challenges facing the public and private sectors. All RAND monographs undergo rigorous peer review to ensure high standards for research quality and objectivity.

Army Network-Enabled Operations

Expectations, Performance, and Opportunities for Future Improvements

Timothy M. Bonds, John E. Peters, Endy Y. Min,
Lionel A. Galway, Jordan R. Fischbach, Eric Stephen Gons,
Garrett D. Heath, Jean M. Jones

Prepared for the United States Army

ARROYO CENTER

The research described in this report was sponsored by the United States Army under Contract No. W74V8H-06-C-0001.

Library of Congress Cataloging-in-Publication Data

Army network-enabled operations : expectations, performance, and opportunities for future improvements / Timothy M. Bonds ... [et al.].
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4683-3 (pbk.)
1. Communications, Military—United States. 2. Information networks—United States. 3. United States. Army—Computer networks. 4. United States. Army—Evaluation. 5. United States. Army—Operational readiness. 6. Command and control systems—United States. 7. Military intelligence—United States. 8. United States. Army—Maneuvers. 9. Logistics. 10. Military art and science—United States. I. Bonds, Tim, 1962-

UA943.A76 2012
355.4—dc22

2009008950

Cover photos courtesy of (top left to bottom right) Spc. Alfredo Jimenz, Jr.; 1st Lt. Tomas Rofkahr; U.S. Army; Russ Meseroll.

Published 2012 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

This monograph documents research that was originally completed in 2008 with the goal of learning lessons from operations in Iraq and Afghanistan about the utility of advanced networks in Army operations. The data and cases used and the findings generated were current as of 2009. Much has occurred since the research was completed, and the Army has applied many of the lessons learned. Importantly, the Army continues to develop and experiment with new networking capabilities. The broad lessons this research identified remain relevant, however, and can continue to inform ongoing Army efforts.

The U.S. Army is investing heavily in networks intended to enable dramatic improvements in operational capabilities. The service is staking much of its future battlefield success on the proposition that units linked together with the appropriate networks can dominate their adversaries. In theory, networked units can know where the other friendly elements are located, share a common understanding of where the enemy is, and be able to devise a plan for raining effects (small arms fire, artillery and mortar fire, perhaps air strikes with precision munitions) on the enemy and destroying him, while at the same time avoiding entrapment by the enemy's maneuvers, thrusts, and parries.

This type of highly accurate and synchronized warfare is difficult; it currently depends on still-emerging communication and information technologies, soldiers mastering complex information management skills, and the integration of both with tactical operations at every echelon. This effort represents a doctrine, organization, training, and materiel modernization on a scale never before attempted. Neverthe-

less, the Army is pushing its way forward, with discrete additions to its networks "spinning off" from research and development programs to be integrated with mature or "legacy" platforms and communication systems. Thus, despite their revolutionary nature, networks are entering the Army's field forces on an evolutionary, incremental basis. In fact, since this research was originally conducted in 2007, the Army has made very significant progress in terms of fielding better networking and communication equipment, training soldiers to leverage networks, and developing doctrine and tactics to employ these new capabilities.

It is the fusion of new networked elements with legacy systems and practices that prompted this study. The questions motivating the research reported here include: How well are the networks performing at the tactical level? How does the hybrid system that results from mating networked and legacy doctrine, organization, training, and materiel perform in the field? Finally, does the network performance currently at the disposal of Army forces in fact deliver significant advantages over the enemy, for example, by allowing Army units to "see first, understand first, act first, and finish decisively"?

The Army Chief Information Officer, G-6, sponsored this research with co-sponsorship from the Army G-3/5/7. The research reported here was performed in RAND Arroyo Center's Force Development and Technology Program. RAND Arroyo Center, part of the RAND Corporation, is a federally funded research and development center sponsored by the United States Army. Questions and comments should be directed to the Program Director, Christopher Pernin, by email to pernin@rand.org, or by telephone at 703-413-1100, extension 5197.

The Project Unique Identification Code (PUIC) for the project that produced this document is SAISZ0747.

For more information on RAND Arroyo Center, contact the Director of Operations (telephone 310-393-0411, extension 6419; FAX 310-451-6952; email Marcy_Agmon@rand.org), or visit Arroyo's Web site at http://www.rand.org/ard/.

Contents

Preface iii
Figures xi
Tables xv
Summary xvii
Acknowledgments xxvii
Abbreviations xxix

CHAPTER ONE
Introduction 1
Study Objective 3
Our Research Approach 3

CHAPTER TWO
A Strategic Context for Understanding the Need for Network-Enabled Operations 5
Tactical Crises in History: Exemplar Cases 5
Today's Tactical Crisis: Identifying and Locating Enemy Forces 8

CHAPTER THREE
Tactical Information: What Commanders and Leaders Need to Know 11
Information Needed for Major Combat Operations 11
Information Needed for Security, Stabilization, and Reconstruction Operations 16
Information Needed for Irregular Warfare 19
Summary 21

CHAPTER FOUR
Network-Enabled Operations 23
What Is the Network? 23
How Is the Network Expected to Help? 26
Metrics for Building Networked and Synchronized Forces 26
Seeing First 28
Understanding First 28
Acting First 29
Finishing Decisively 30
Evaluating Network Performance 30

CHAPTER FIVE
Military Utility of Network-Enabled Operations: Qualitative Assessment of Recent Case Studies 33
General Observations 33
On the Advance: The Drive to Baghdad in Operation Iraqi Freedom 34
The 507th Maintenance Company 36
Company C/1st Battalion, 2nd Marine Regiment 38
3rd Battalion, 69th Armored Regiment, at Objective Peach 40
Convoys and Patrols: The 2nd Squadron, 4th Platoon of the Military Police Company, at the Palm Sunday Ambush 41
Army Combat Outpost: Defense, Overwatch, and Relief 44
Combat Reconnaissance: 1-3rd Special Forces Group at Syahcow 47
Counterambush: Manned-Unmanned Aircraft Teaming with Ground Forces 49
1-24th: Shadow UAS, Strykers, and Joint Coordination Center 50
TF 3-29th: F-15Es, Predator UAS, 101st Airborne (Air Assault), and the Balad Air Base Joint Defense Operations Center 51
Scouts, Hunters, and the Brigade Tactical Operations Center 51
5-73rd: Helicopters, Warrior UAS, and Brigade HQ 51
Task Force ODIN 52
DCGS-A, the "Flat Network," and Intelligence Support to BCTs and Below 54
Summary Observations 57

CHAPTER SIX
Military Utility of Network-Enabled Operations: Quantitative Assessment of Training and Operational Experiences 59
Trends from Iraq 60
NTC and JRTC Training Data 63

CHAPTER SEVEN
Military Utility of Network-Enabled Operations: Officer Impressions of Network Functionality 65
Discussion of First Survey Results 65
The Survey Population 66
Assessments of Network Performance 67
Evaluation of Network Performance Metrics 68
Main Threads of Individual Officer Comments 69
Overall Impressions of Network Performance 69
Discussion of Second Survey Results 70
What Do the Survey Results Say About the Physical Domain? 72
Summary of the Physical Domain 73
The Physical Domain Is Not Adequate to Deliver See First Capabilities to the Officers 73
What Do the Survey Results Say About the Information Domain? 76
Summary of the Information Domain 76
What Do the Survey Results Say About the Cognitive Domain? 80
Summary of the Cognitive Domain 81
What Do the Survey Results Say About the Social Domain? 87
Summary of the Social Domain 88
The Social Domain Needs to Better Include Coalition and Host Nation Partners in the Information Exchange 88
Summary of the Survey Results 90
Does Better-Quality Networking Lead to Improved Information-Sharing? 91
Does More Information-Sharing Lead to Improved Information Quality? 92
Does More Information-Sharing Lead to Improved Individual Understanding? 92

Does More Information-Sharing Lead to Improved Shared Understanding? 92
Does Improved Individual Understanding Lead to Improved Decisionmaking? 93
Does Improved Shared Understanding Lead to Improved Decisionmaking? 93

CHAPTER EIGHT
Options to Enhance Network Performance 95
Observations from Case Studies, Data Mining, and Surveys 95
The Network's Strong Suit 95
Where the Network Proves Less Capable 96
Network Performance "Bottlenecks" 97
New Army and DoD Initiatives 97
Informal Networks 98
Self-Synchronization 99
Electronic Overwatch 102
Applying Self-Synchronization and Electronic Overwatch 104
Counterfactual: Application of Self-Synchronization and Electronic Overwatch to Historical Cases 106
The 3-69th Armor 106
Company C/1-2 Marines 107
507th Maintenance Company 107
2/4/617th MP Company 108
2/C/1-24th Infantry 109
1-3rd SFG 109
Summary of Potential Network-Enabled Improvements 109
Potential DOTMLPF Changes to Improve Networks 110
Doctrine 110
Organization 111
Training 111
Materiel 111
Leadership and Personnel 113

CHAPTER NINE
Military Utility of Network-Enabled Operations: Conclusions and Recommendations 115
Conclusions 115
Army Networks Enabled the "Quality of Firsts" for Senior Army Tactical Echelons During Major Combat Operations 115
Army Networks Have Not Yet Enabled the Same "Quality of Firsts" for SSTR, COIN, and Irregular Warfare Operations 116
Soldiers and Leaders Are Informally Linking Networks Together to Enhance Their Effectiveness 117
Opportunities Are Emerging for the Army to Enhance Future Operations 117
Recommendations 119
Continue and Expand Efforts to Extend the Network to Lower Echelons 119
Invest More Time in Developing and Exploiting Informal Networks 120
Expand the Network to Include All Important Actors 120
Enact DOTMLPF Changes to Enable Self-Synchronization and Electronic Overwatch 121

APPENDIXES
A. Officer Impressions of Network Performance 123
B. Officer Impressions of the Performance of Network Programs of Record 133
C. Statistical Analysis of Officer Impressions of Network Functionality 157
D. Statistical Analysis of Unit Performance Data from the National Training Center 183

Selected Bibliography 193

Figures

5.1. Actions of the 3-69th Armor, C/1-2 Marines, and 507th Maintenance Company During Advance on Baghdad 36
5.2. Actions of the 2/4/617th Military Police (MP) Company at the Palm Sunday Ambush 42
5.3. Actions of the 1-24th Infantry Battalion (Stryker) in Mosul 45
5.4. Actions of the 1-3rd SFG at Syahcow 48
6.1. Average U.S. Casualties per Month from IEDs, 2003–2007 61
6.2. Violence Indicators in Iraq 62
7.1. Distribution of Overseas Tours Among Respondents 67
7.2. How Reliably Could You Reach Other Units Using Voice or Text? 74
7.3. Percentage of Respondents Who Marked N/A 75
7.4. Reach Reliability with Contractors/NGOs and Host Nations Improved 75
7.5. Quality Comparisons of Formal and Informal Information .. 77
7.6. Completeness of and Confidence in Information, by Rank 78
7.7. Timeliness and Relevance of Information, by Rank 79
7.8. Reasons for Using Informal Network, by Branch 80
7.9. How Important Was the System to Your Situational Understanding? 82
7.10. How Important Was the System to Your Decisionmaking Process? 83
7.11. How Often Did This System Help You Make Your Decision Faster Than You Would Have Without the System? 84

7.12. How Important Was the System in Raising Your Confidence That Your Decision Was a Correct One? 85
7.13. How Important Was the System to Your Decisionmaking Process? 86
7.14. To What Degree Was the System User-Friendly? 87
7.15. How Reliably Did the System Facilitate Sharing of Information with Other Units? 89
7.16. How Often Did This System Establish Shared Understanding? 90
8.1. Synchronizing the Operations of Subordinate, Adjacent, and Joint Forces 105
C.1. Distribution of Overseas Tours Among Respondents 158
C.2. How Reliably Could You Reach Other Units Using Voice or Text? 162
C.3. Percentage of Respondents Who Marked N/A 163
C.4. Reach Reliability with Contractors/NGOs and Host Nations Improved 163
C.5. Voice Reach, by Rank 164
C.6. Voice Reach, by Branch 164
C.7. Text Reach, by Rank 165
C.8. Text Reach, by Branch 165
C.9. Did the Capabilities of the Network Devices Slow Down Your Work? (by Rank) 167
C.10. Did the Capabilities of the Network Devices Slow Down Your Work? (by Branch) 168
C.11. Quality Comparisons of Formal and Informal Information 169
C.12. Completeness of and Confidence in Information, by Rank 170
C.13. Timeliness and Relevance of Information, by Rank 170
C.14. Reasons for Using Informal Network, by Branch 172
C.15. How Important Was the System to Your Situational Understanding? 173
C.16. How Important Was the System to Your Decisionmaking Process? 174
C.17. How Often Did This System Help You Make Your Decision Faster Than You Would Have Without the System? 175

C.18. How Important Was the System in Raising Your Confidence That Your Decision Was a Correct One? 176
C.19. How Important Was the System to Your Decisionmaking Process? 177
C.20. To What Degree Was the System User-Friendly? 178
C.21. How Often Did Other Units Push Information to You or How Often Did You Push Information to Others? 179
C.22. How Often Did Other Units Push Information to You or How Often Did You Push Information to Others? 180
C.23. How Reliably Did the System Facilitate Sharing of Information with Other Units? 181
C.24. How Often Did This System Establish Shared Understanding? 182

Tables

4.1. Knowledge Components of See First, Understand First, Act First, and Finish and Decisively for Different Types of Operations 27
5.1. Summary of Unit Awareness and Synchronization in Historical Cases 58
7.1. Survey Respondent's Military Occupational Specialty 66
7.2. Overall Network Evaluations 67
7.3. Summary of Average Network Performance, by Metric 68
7.4. Eligible Respondents, by Rank 70
7.5. Eligible Respondents, by Branch 71
7.6. Distribution of Officer Deployment to Iraq and Afghanistan 71
7.7. Qualitative Descriptions of the Quantitative 1-to-5 Scale 72
7.8. Correlations Between Cognitive Domain Attributes and System User-Friendliness 86
8.1. Potential for Networks to Improve Unit Awareness and Synchronization in Historical Cases 110
B.1. Sample Frame of Officers in Selected Ranks and Branches 134
B.2. Final Strata and Sample Sizes 135
B.3. Formal System Strata Sample Frame 138
B.4. List of Formal Systems, by Respondent's Branch 141
B.5. Response Rates for All Respondents and Eligible Respondents, by Rank 144
B.6. Response Rates for All Respondents and Eligible Respondents, by Branch 144
B.7. Percentage Response Rates, by Branch and Rank 145

C.1. Survey Respondent's Military Occupational Specialty..... 157
C.2. Mean Network Evaluations..... 159
C.3. Summary of Network Performance Metrics..... 159
C.4. Response Rates, by Rank..... 160
C.5. Response Rates, by Branch..... 161
C.6. Officer Deployment Distribution to Iraq and Afghanistan..... 161
C.7. Qualitative Descriptions of the Quantitative 1-to-5 Scale..... 162
C.8. Ranks and Branches with Highest Ratings for Reach by Voice and Text..... 166
C.9. Network Flexibility, Capacity, and Responsiveness, by Rank and Branch..... 167
C.10. Was Your Operation Affected by the Limited Number of Radios, Phones, and Computers?..... 168
C.11. Correlations Between Device Quality and Reach..... 169
C.12. Signal Gave Highest Ratings to Information Quality..... 171
C.13. Reasons for Using Informal Network..... 171
C.14. How Often Did You Understand All of the Information That You Needed to Accomplish Your Task? (by Rank)..... 171
C.15. How Often Did You Understand All of the Information That You Needed to Accomplish Your Task? (by Branch)..... 172
C.16. Formal System Function in Officer Situational Understanding..... 173
C.17. Correlations Between Cognitive Domain Attributes and System User-Friendliness..... 174
D.1. Questions on the Use of Digital C4ISR Systems for Each Level of Unit..... 184
D.2. Overall Performance Versus Use of Digital C4ISR..... 186
D.3. Phi Coefficient for Company Performance Rating Versus Use of Digital C4ISR Systems..... 188
D.4. Phi Coefficient for Platoon Performance Rating Versus Use of Digital C4ISR Systems..... 190

Summary

The U.S. Army expects that the performance of ground forces can be greatly enhanced by improving the networks that tie them together—and by developing new tactics that take advantage of the special properties of these networks. The Army employs literally thousands of individual networks, including those used by the operating forces for command and control, intelligence, maneuver, fires, and logistics, as well as those used by the generating force at bases in the continental United States and abroad.[1] These networks include the infostructure and services that process, store, and transport the information used by the Army.[2] Ultimately, then, these networks extend into the minds of soldiers and leaders and into their interactions with each other. In this monograph, we examine the capabilities that this broad set of networks provides in four areas:[3]

- physical aspects, including the radios, terminals, routers, landlines, and so forth that constitute the network infrastructure and provide network connectivity
- the information environment, including the databases where information is created, manipulated, and shared

[1] LandWarNet is the name that the Army uses for all of its networks (see Boutelle, 2004).

[2] U.S. Army Training and Doctrine Command (TRADOC) (2006a).

[3] TRADOC groups the first two categories into the Technical Area, and the third and fourth categories into the Knowledge Area (see Vane, 2007). These areas closely compare with the domains described by Alberts, Gartska, and Stein (1999).

- cognitive attributes, including sense-making tools that aid or enable situational awareness, situational understanding, decision-making, and planning
- social interaction, including collaboration, synchronization of actions, standard operating procedures, and tactics, techniques, and procedures enabled by the network.

One advantage that the Army hopes to gain from improved networks is the "quality of firsts," the ability to "see first, understand first, act first, and finish decisively." This concept entered development when the U.S. military was focused on major combat operations (MCOs). This study also assessed the degree to which networks can provide these same qualities to stability, security, transition, and reconstruction (SSTR) operations, counterinsurgency (COIN) operations, and warfare against irregular forces.

Specifically, this study addressed the following questions:

- Do the networks used by the Army enable commanders to "see first, understand first, act first, and finish decisively" and otherwise get forces and effects to the right place at the right time?
- What new, and perhaps unexpected, developments should the Army embrace and push forward?
- Where (that is, in what areas of the network) would additional investments yield the greatest rewards in terms of added performance?
- What changes in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) should the Army make to achieve the expected network functionality and utility?

Conclusions

Our analysis of operations in Iraq, unit performance at the National Training Center and Joint Readiness Training Center, and officer impressions of network functionality led us to the following conclusions.

Army Networks Enabled the "Quality of Firsts" for Senior Army Tactical Echelons During Major Combat Operations

The ability of U.S. forces to gather, process, and disseminate battlespace information in a networked fashion has given them a tremendous advantage in MCOs. This dominant battlespace information has allowed U.S. forces to move faster and apply military power more aggressively and more effectively than their adversaries. Today's networks enable several key operational capabilities:

- shared situational awareness of U.S. forces, although a current or complete red picture was sometimes not available to echelons below brigade
- unity of action between U.S. forces
  - superior coordination and synchronization of U.S. forces when on the offensive—that is, when they have the initiative
  - promising instances of excellent coordination and synchronization when reacting to enemy actions or attacks
- enhanced shared understanding.

The most significant problem noted during past MCOs was an incomplete or dated view of red forces. New investments, such as unmanned aircraft systems and the Distributed Common Ground System–Army (DCGS-A), may help to improve red force information available to lower echelons.

Army Networks Have Not Yet Enabled the Same "Quality of Firsts" for SSTR Operations, COIN, and Irregular Warfare

Today's networks do not yet enable all of the force-enhancing effects that the Army expects:

- Army units often do not see first or act first when enemies use irregular tactics.
  - Many reconnaissance, surveillance, and information systems were developed to find conventional armies when U.S. forces have the initiative.

  - They are less effective in detecting and identifying irregular enemies before they initiate attacks.
  - Information superiority in COIN and irregular warfare can therefore shift from U.S. forces to insurgents.

The Army's current networks do not yet enable seeing first or understanding first in all SSTR, COIN, and irregular warfare operations. The networks enable situational awareness of other blue units but do not always provide reliable awareness of red units before they attack, which is much more challenging. The networks do generally support reactive tactical coordination and unity of action, thereby allowing units to usually finish decisively.

Soldiers and Leaders Are Informally Linking Networks Together to Enhance Their Effectiveness

Our officer survey data revealed the following:

- Informal networks—often hosted on SIPRNet (Secret Internet Protocol Network)—received the highest ratings of all the networks.
- SIPRNet was rated as better than the other systems at establishing shared situational awareness with U.S. forces.
- But key systems—e.g., SIPRNet, FBCB2 (Force XXI Battle Command Brigade and Below), and CPOF (Command Post of the Future)—are not typically shared with coalition and host nation units.

Officers we surveyed viewed the SIPRNet as the best tool for establishing situational awareness between U.S. units. Where available, the SIPRNet was an essential means of connecting soldiers and leaders with sensitive databases and other sources of information within theater or elsewhere in the world. Unfortunately the SIPRNet and other networks such as FBCB2 are not typically shared with coalition or host-nation units nor are network-enabled tools such as CPOF.

The case studies and surveys we conducted reveal that soldiers and leaders are investing time and unit resources in informal networks that connect and fill gaps in the formal networks. These include unit-

level databases to gather information from (and for) local operations; user applications to sort, search, and make sense of these data (that is, cognitive aids); and social networks to share this knowledge with peers brigade-, division-, and corps-wide. The blogs, online discussion groups, and chat rooms prompted by such shared application have spawned an important "social domain" of the network to enhance the effectiveness of unit, task-force, or theater-wide operations.

Opportunities Are Emerging for the Army to Enhance Future Operations Through Improvements in the Networks' Social and Cognitive Domains

We saw significant potential to enhance the effectiveness of U.S. and coalition forces by providing networks that can enable

- adjacent U.S. units to self-synchronize
- command posts and higher headquarters to provide "electronic overwatch."

As noted in this monograph, ground forces are putting more and more information onto SIPRNet, FBCB2, CPOF, and other networks that can be used to synchronize the operations of adjacent units and units that are moving adjacent to one another. Often, this information can be updated automatically, without placing additional obligations on already overtaxed command post staffs. For example, the movement tickets that convoys are supposed to generate before departure could be pushed automatically to the headquarters of each area of operation (AO) that a convoy will move through. These trip tickets, along with information broadcast en route over SLANT reports, would provide a way to synchronize the convoy with those forces it will move adjacent to. Similarly, any moving air or ground unit could synchronize its activities with other U.S. forces that it approaches in the battlespace.

Additional advantages may be gained when networks enable electronic overwatch. Command posts that are synchronized with lower-echelon forces in their areas of operation may be in the best position to provide support (such as intelligence, fire support, or even a quick-reaction force) to these forces when they most need it. Having the nec-

essary connections, tools, knowledge, and mindset may allow these command posts to enhance the effectiveness of these units at critical moments.

Recommendations

The Army has made substantial investments in the network with the intention of achieving network-enabled operations. Indeed, the rubric "see first, understand first, act first, and finish decisively" has become pervasive in current and future concepts. Assuming that the Army continues to believe that the network and network-enabled operations can deliver enhanced battlefield performance, we recommend that the Army pursue the network objectives described below.

Continue and Expand Efforts to Extend the Network to Lower Echelons

At the tip of the spear, small units experience limited network access and capabilities. Often, platoons and squads are operating on the move or in combat outposts far from other units and lack direct access to intelligence, surveillance, and reconnaissance data. Current plans to distribute unmanned aerial vehicles (UAVs) downward through the brigade combat teams are a step in the right direction, along with direct-downlink terminals. In addition, providing the DCGS-A down to battalion and company levels will help. The key future challenge will be maintaining these connections to units on the move and building display systems that enhance effectiveness during high-intensity operations. More recent initiatives to provide Human Terrain Teams, Cryptologic Support Teams, and other specialized support at echelons brigade and below should be continued.

Many of the officers who responded to the project's surveys called for forward distribution of a SIPRNet-like Web-based classified system to lower-echelon units. SIPRNet is now reaching some company-level units at fixed sites, but platoons are increasingly assigned to man remote outposts. Where appropriate, the Army should develop the means to provide secret channels down to the lowest level of iso-

lated units. Where this is not possible (because of operational security [OPSEC] concerns, limited bandwidth, and so forth), their higher headquarters should provide electronic overwatch.

One aspect of extending the network should be to extend its capabilities to identify the enemy before the shooting starts. The Army should intensify its efforts to expand its reconnaissance tools. In addition to the efforts under way, the Army might also consider emblematics, more biometrics, and new ways of instrumenting the battlespace that would reveal enemy combatants and their organizations. Another aspect of extending the network would be to take advantage of current intelligence, surveillance, and reconnaisance "feeds" by distributing them down the chain of command to smaller units that could use this information as context for understanding the clues they are collecting about the enemy within their own area of operations.

Invest More Time in Developing and Exploiting Informal Networks

Officer survey responses indicate that informal networks perform important functions within and among deployed units. It appears that they may fill gaps in information and connectivity not provided by the formal network. The Army has supported some of these soldier initiatives—and should strive to study and harness these networks as they emerge. The G-6 and G-3 will want to coordinate closely to begin thinking about how to manage the intersection of systems of record with informal networking practices and how insights from such a process might inform network design and battle command practices.

Expand the Network to Include All Important Actors

A central tenet of irregular warfare is that the military provides only part of the solution. The host nation, coalition partners, other U.S. executive branch agencies (such as the State Department and U.S. Agency for International Development), international agencies, and nongovernmental organizations (NGOs) must be included. Expanding the network to include such a wide range of coalition partners clearly presents issues about OPSEC and information security, but there are some precedents for handling them. The Combined Enterprise Regional Information Exchange (CENTRIX) network, despite its limitations,

suggests one way to undertake extended connectivity and share "rapid decay" current intelligence, since it makes enemy exploitation of leaked intelligence difficult. This would also promote unity of effort and good faith with any number of participants.

Still, some nations, NGOs, and individuals may require extensive vetting over considerable periods of time. It may be necessary to continue the Special Forces practice of using unclassified, commercial radios and computers to connect these groups and individuals with U.S. forces—recognizing that these communications are very likely to be intercepted.

Enact DOTMLPF Changes to Enable Self-Synchronization and Electronic Overwatch

The Army should consider the following DOTMLPF changes to implement our recommendations:

- Doctrine
  - Help platoons and squads when they are operating alone against irregular or hidden forces. Doctrine needs to allow and encourage adjacent units to self-synchronize information, plans, and capabilities while executing their assigned missions.
  - Assign overwatch duty to an adjacent unit when it is in a tactical situation that allows it to provide support.
- Organization
  - Provide designated headquarters and command posts with the appropriate staff, network tools, and training to conduct electronic overwatch.
- Training
  - Provide training to implement self-synchronization and electronic overwatch.
- Materiel
  - *SIPRNet:* Provide SIPRNet down to the platoon level if these echelons continue to man combat outposts.
  - *Blue force location, identification, tracking, and synchronization:* Provide real-time blue force tracking to every unit that con-

ducts independent operations. (Also, provide the best red force picture possible on this equipment.)
  - *Intelligence, surveillance, and reconnaissance systems:* Continue to provide an organic way to access intelligence, such as direct unmanned aircraft system downlinks and DCGS-A. Enable electronic overwatch over voice and text systems for those echelons not able to receive DCGS-A.
- Leadership and Personnel
  - Encourage soldiers and leaders to develop and use such sites as the CompanyCommand Forum and CavNet as places to meet, learn, and build new concepts.
  - Reward soldiers and leaders who develop new applications to tap into the multitude of classified databases to gather intelligence concerning recent enemy movements, attacks, and other activities.

Acknowledgments

We are indebted to a number of people for their help with this project. First, we were fortunate to have the direct involvement of two RAND Army fellows during 2006–2007, LTC Jean Jones and LTC Garrett Heath, whose participation added clarity and focus to the research. We enjoyed the very helpful advice of our project sponsors Major General Conrad Ponder, then–Major General Gerety, and Dave Shaddrix, as well as our action officer LTC Hattie Bouyer in Headquarters, Department of the Army, Office of the Chief Information Officer/G-6. We are indebted to James Cooke and Colonel Chris O'Connor, G-3, who engaged constructively with the project team and helped us sharpen our thinking. We thank Anna Waggener at the Army War College for her assistance with the administering of our survey to War College students. We also thank LTC Thomas Rivard, Walter Thompson, A. J. Luker, and Rhonda Langford for their help with our survey of officers attending the Command and General Staff College, School of Advanced Military Studies, the Infantry Officers Advanced Course, and the Field Artillery Officer Advanced Course, respectively.

Finally, we would like to acknowledge several colleagues who helped us in our research and analysis. First, we thank our reviewers Stuart Johnson of RAND and Irving Lachow of the National Defense University. We also thank Stuart Starr of the National Defense University for his comments on an early draft of this monograph. These colleagues helped strengthen our document with their many insightful comments and suggestions. We also benefited from discussions with our program director at the time, Bruce Held, and RAND colleagues

Leland Joe, Louis Moore, Isaac Porche, Daniel Gonzales, and Lionel Galway.

Abbreviations

ABCS	Army Battle Command System
ADJ	adjacent unit
AFATDS	Advanced Field Artillery Data System
AIF	anti-Iraqi force
AO	area of operation
AOR	area of responsibility
AR	Armor
ASAS	All Source Analysis System
ATO	air tasking order
BCS3	Battle Command Sustainment Support System
BCT	Brigade Combat Team
BFT	Blue Force Tracker
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CAB	Combat Aviation Brigade
CAS	close air support

CENTRIX	Combined Enterprise Regional Information Exchange
CFLCC	Combined Force Land Component Command
CIA	Central Intelligence Agency
CIDNE	Combined Information Data Network Exchange
CIO	Chief Information Officer
C/N	contractor/NGO
Co	coalition unit
COIN	counterinsurgency
CONOP	concept of operations
CONUS	continental United States
COP	common operational picture
CPOF	Command Post of the Future
CSS	combat service support
DCGS-A	Distributed Common Grounds System–Army
DCGS	Distributed Common Grounds System
DoD	Department of Defense
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
EBR	Evidence Based Research
EPLRS	Enhanced Position Location Reporting System
FA	Field Artillery
FBCB2	Force XXI Battle Command Brigade and Below
HI	higher unit

HN	host nation
HQDA	Headquarters, Department of the Army
HUMINT	human intelligence
ID	Infantry Division
IED	improvised explosive device
INF	Infantry
ISR	intelligence, surveillance, and reconnaissance
ISYSCON	Integrated System Control
JADOCS	Joint/Automated Deep Operating Coordination System
JDLM	Joint Deployment Logistics Model
JDOC	Joint Defense Operations Center
JIOC-I	Joint Intelligence Operating Capability–Iraq
JNN	Joint Network Node
JRTC	Joint Readiness Training Center
JSTARS	Joint Surveillance and Target Attack Radar System
MCO	major combat operation
MCS	Maneuver Control System
MEF	Marine Expeditionary Force
mIRChat	Internet Relay Chat
MOS	military occupational specialty
MP	Military Police
MTS	Mobile Tracking System
NATO	North Atlantic Treaty Organization

NGO	nongovernmental organization
NTC	National Training Center
ODA	Operational Detachment–Alpha
ODS	Operation Desert Storm
OIF	Operation Iraqi Freedom
OMF	Officer Master File
OPSEC	operational security
ORD	Ordnance
QM	Quartermaster
QRF	quick-reaction force
RPG	rocket-propelled grenade
RSTA	reconnaissance, surveillance, and target acquisition
S-2/G-2 staff	Intelligence Staff
S-6/G-6 staff	Information Management Staff
SFG	Special Forces Group
SIG	Signal
SIGINT	signals intelligence
SIPRNet	Secret Internet Protocol Network
SOF	Special Operations Forces
SOP	standard operating procedure
SSTR	security, stability, transition, and reconstruction
SUB	subordinate
TAIS	Tactical Airspace Integration System
TBM	theater ballistic missile

TF	Task Force
TF ODIN	Task Force Observe, Detect, Identify, and Neutralize
TOC	Tactical Operations Center
TRADOC	Training and Doctrine Command
TRN	Transportation
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
UAV	unmanned aerial vehicle
ULLS	Unit Level Logistics System
USAF	U.S. Air Force
USCENTCOM	U.S. Central Command
USMC	U.S. Marine Corps
VBIED	vehicle-borne improvised explosive device
VoIP	voice over Internet protocol
VSAT	very small aperture terminal
WMD	weapons of mass destruction

CHAPTER ONE

Introduction

The U.S. Army is investing heavily in networks—including the technology to bring them to fruition and the practical steps necessary to embed them in tactical Army units. The concept of network-enabled operations and the power it potentially brings to the battlefield was developed when the U.S. military's focus was still very much on major combat operations (MCOs). This study assessed the utility of that concept as the Army moves to a combination of MCOs; stability, security, transition, and reconstruction (SSTR) operations; counterinsurgency (COIN) operations; and irregular warfare operations.

The latter kinds of operations have posed very different challenges from MCOs and have proven *not* to be lesser-included cases. In MCOs, the ability to gather, process, and disseminate battlespace information in a networked fashion has given U.S. forces a tremendous advantage. Superior battlespace information has allowed the Army to move faster and to apply military power more aggressively and more effectively than its adversaries. In SSTR and COIN operations, information dominance can shift to the insurgents who blend in with the local population, speak the local language, understand the local culture, and, in general, "know the turf." This is a tough problem for the Army, since populating the "red" part of situational awareness has become highly elusive.

To fulfill the vision that its soldiers must dominate their adversaries on any future battlefield, the Army has high expectations for the capabilities that its networks will deliver:

- "Networked" units will know their position in the battlespace and the relative locations of friendly units, and they will share a perception of where the enemy lurks.
- This "situational awareness" will allow Army leaders at all levels to dominate their adversaries—either by destroying them through decisive action or by avoiding an engagement under unfavorable circumstances—as the situation dictates.
- Taken together, meeting these expectations will provide the "quality of firsts," which includes the ability to
  - see first
  - understand first
  - act first
  - finish decisively.

One of the most striking features of recent operations in Iraq and Afghanistan is the degree to which battalions and companies, and sometimes even platoons and squads, operate on their own—away from immediate reinforcement or support from their parent units. Given the degree to which Army forces—most especially small units—have been tested, it is appropriate for the Army to assess how well its networks are meeting the expectations described above and whether the networks are delivering the military utility that Army officials had hoped they would. It should now be possible to answer such questions as:

- Do the Army's networks help commanders to see first, understand first, act first, and finish decisively and otherwise get forces and effects to the right place at the right time?
- What new, and perhaps unexpected, developments should the Army embrace and push forward?
- Where (that is, in what network features) would additional investments yield the greatest rewards in terms of added performance?
- What changes in doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) should the Army make to achieve the expected network functionality and utility?

Study Objective

This study assessed how well the current set of networks used by the Army help achieve the "quality of firsts" and otherwise get forces and effects to the right place at the right time within the battlespace.[1] The resulting assessment is intended to help the Army decide where (that is, in what areas of the network) additional investments might enable even greater force effectiveness.

Our Research Approach

The first step in our analysis was to describe the historical context for understanding the U.S. military's current problems in finding elusive enemy forces (Chapter Two). We then describe the tactical information that commanders need to find, identify, and target these enemy forces and accomplish current and future missions (Chapter Three). The first part of this monograph concludes with a description of the Army's networks and how they are expected to enable successful operations (Chapter Four).

The next three chapters evaluate the extent to which current networks have actually enabled the Army's operations. The Army has amassed a vast body of unit after-action reports that describe experiences from the corps to the squad level at different points in time. We used these after-action reports to construct a series of case studies from the historical record to help illustrate various attributes of network performance, both in instances in which the network performed brilliantly and in other instances in which its contributions were much less helpful (Chapter Five).

We also made use of the growing body of data concerning unit performance during training and actual operations. Training statistics

[1] In this monograph, we frequently address those capabilities that Army forces need and what the Army should do to provide them. We recognize that these same capabilities may also be needed by joint forces and may often be provided by the other services. Although our aim is to advise the Army regarding what it should do, we also acknowledge that our advice might often be appropriate for the other services as well.

provide some clues into the ways in which the network has enhanced unit performance at the National Training Center (NTC) and the Joint Readiness Training Center (JRTC). We also mined several databases from ongoing operations in Iraq and Afghanistan to measure the differences in operational performance between the early deployed, less network-enabled units and, later, the fully network-enabled successor units (Chapter Six).

Finally, there are thousands of serving officers with first-hand experiences with the Army's networks gained during multiple combat tours. We surveyed officers who had served in Iraq or Afghanistan to capture their impressions of Army networks. This survey asked about network reliability (Did it work when I needed it?), connectivity (Could I contact the organizations and individuals essential to my mission?), content (Could I access the facts and data I needed?), and functionality (Could I organize and manipulate facts and data to achieve awareness and understanding?).[2] Chapter Seven summarizes the impressions of network performance from our survey of Army officers.

Chapter Eight offers some options for improving future networks to overcome the limitations identified in the preceding chapters. Potentially high-payoff network improvements are proposed in terms of changes to DOTMLPF. Chapter Nine offers our conclusions and recommendations for the Army.

---

[2] Once the research began, we realized that we needed two separate surveys: one to capture macro-level impressions of network performance and a second, more detailed survey to track the performance of the systems of record that constitute the material-technical domains of the network. The details of each survey appear in Appendixes A and B, respectively.

CHAPTER TWO

A Strategic Context for Understanding the Need for Network-Enabled Operations

From time to time throughout history, armies have faced tactical crises of strategic importance. The strategic importance typically derived from the fact that the tactical problem threatened to make an army's defeat mechanism—the tactics, techniques, and procedures (TTPs) that produced success—obsolete. Armies have either found new approaches to solving these tactical crises or they have suffered the (sometimes disastrous) consequences.

As we describe below, the U.S. Army faces a tactical crisis today. The Army expects to employ network-enabled forces to solve this problem and has developed a concept of network-enabled operations through experimentation, modeling and simulation, and the study of unit case histories. This chapter offers some context for understanding the role that the Army hopes the network will play in enabling future operations.

Tactical Crises in History: Exemplar Cases

In the latter half of the 19th century, European armies struggled to respond to the expanding killing zone their forces had to cross to close with and destroy the enemy. (Closing with and then destroying enemy forces was the preferred defeat mechanism of the day.) The advent of magazine-fed rifles, machine guns, rapid-firing field artillery, and smokeless gunpowder combined to expand the killing zone of the battlefield by an order of magnitude. Instead of infantry having to charge across several hundred meters in the final assault, the killing zone had

expanded to 2,000 meters and was much more lethal, with the promise of withering combined arms fire from the enemy. The potential casualties from such a clash would be impossible to sustain, leading to the prospect that European armies might become obsolete.

European armies grappled with the problem by redefining the role of cavalry (which eventually led to the tank), adopting a counterbattery role for the artillery, and exploring opportunities to employ air power.[1] Indeed, before World War I, some authorities hoped that air power would deliver the common operating picture that many commanders today hope the network will provide.[2]

Following World War I, Blitzkrieg evolved to address a new tactical crisis: how to deal with massive, fixed fortifications (the Maginot Line) and overcome a numerically superior adversary (soon to be the allied powers of World War II).[3] Ultimately, Blitzkrieg was able to circumvent the Maginot Line, cause the French to surrender, drive the British Expeditionary Force into the sea at Dunkirk, and force a Russian retreat to the gates of Moscow. However, it proved not to be quite the defeat mechanism Hitler thought it was. It could not compel British Prime Minister Winston Churchill to ask for truce terms following the calamity of May 1940. Without secure sea lines of communication, Blitzkrieg could not stop British Field Marshal Bernard Montgomery at el Alamein.[4] Nor, finally, could Blitzkrieg make up for the sheer size of the Soviet Union, with its vast strategic depth and almost equally vast Red Army.[5] The Wehrmacht's experience, then, illustrates what happens when an army faces a tactical crisis and reaches a mistaken—or only partially correct—conclusion about an appropriate remedy.

During the Cold War, the North Atlantic Treaty Organization (NATO) members faced a tactical crisis about how to cope with the

---

1 Echevarria (2000, Chapters 1–3).

2 Echevarria (2000, p. 168).

3 Corum (1992).

4 The Afrika Korps slowly starved for critical supplies as the Western powers used Malta as a secure base from which to destroy German shipping, thus depriving German and Italian forces in North Africa of vital food, fuel, ammunition, and spare parts.

5 Von Mellenthin (1971).

daunting size of the Soviet Union and Warsaw Pact armed forces. At the Lisbon summit in 1952, the allies concluded that they would need on the order of 90 divisions—a force that would be ruinously expensive for the still-struggling economies of Western Europe, which had yet to recover fully from the effects of World War II.[6] Nuclear weapons—including tactical nuclear weapons—became the prescription by the late 1960s. The thinking was that, given the limitations on the alliance's conventional forces, NATO could avoid war with the East altogether by deterring Moscow with the sum of allied military might and an escalation ladder (a sequence of increasingly severe military options) that extended from its conventional forces to its tactical nuclear weapons all the way up to the strategic arsenal.

Fortunately, we do not know how effectively nuclear weapons performed in shoring up NATO's defeat mechanism. Other forces helped to bring the Cold War to its conclusion. Even during the era of East-West confrontation, however, some authorities expressed misgivings about NATO's strategic posture. Would Washington really sacrifice Chicago for Paris if it came to that? These misgivings suggest—albeit inconclusively—that nuclear weapons may not have been a completely satisfactory tool to address NATO's tactical crisis: insufficient conventional forces to defeat the Soviet–Warsaw Pact colossus. (Furthermore, we observe that the United States and its NATO allies eventually spent considerable sums to modernize and grow their conventional forces, particularly in the decade from the mid-1970s to the mid-1980s.)

We will mention one more tactical crisis—one that first emerged during Operation Desert Storm (ODS), continued through subsequent operations, and still exists today. That tactical crisis is the great difficulty in finding and destroying, neutralizing, or seizing strategically important weapons, operations, or enemy leaders.

The first such example in recent campaigns occurred during ODS, when Iraq fired theater ballistic missiles (TBMs) against civilian targets in Israel and Saudi Arabia. At that time, Iraq was known to

[6] Haftendorn (2005). See also NATO (1952), especially paragraph four of the communiqué. See also NATO (1955), which acknowledges explicitly the alliance's dependence on nuclear weapons.

be capable of delivering chemical weapons; it had killed thousands of Iranians and Kurds in this fashion. Several bad strategic outcomes—from a U.S. point of view—seemed possible as a result of this Iraqi strategy. Israel might have attacked Iraq in some way and thereby driven a wedge between the United States and its Arab allies. Or, those Arab nations hosting U.S. forces or contributing their own units might have chosen to settle with Iraq rather than suffer the losses caused by a continuing TBM barrage—particularly if those TBMs might be armed with weapons of mass destruction (WMD). Finally, the TBM attacks might have caused serious loss of life among civilians and military personnel and damage to facilities and equipment.

In response, the United States mounted an enormous air effort, deployed air defense assets (especially the Patriot system) to intercept the TBMs, and sped up programs to improve the capabilities of defensive systems. Ultimately, neither the TBMs nor the counter-TBM operations proved to be militarily effective, although each had important political and psychological effects during the conflict.

The tactical problem of finding particularly important targets—TBMs, air defenses, leadership elements, or WMD—has also been a dominant feature of subsequent operations, including those in Somalia (leadership), Serbia and Kosovo (SA-6 surface-to-air missiles and marauding ground forces), Afghanistan (leadership), and Iraq both during the major combat operations phase (leadership, TBMs, and WMD) and in the subsequent stability operations (insurgents).

Today's Tactical Crisis: Identifying and Locating Enemy Forces

The U.S. Army faces a tactical crisis in its campaigns in Iraq and Afghanistan today: It has difficulty finding its enemies and separating civilians from foes.[7] The Army has incomplete information tools to help it identify enemy combatants and separate them from an otherwise

[7] See Tyson and Kessler (2007, p. A11).

peaceful population.[8] As a result, Army units cannot, on their own, adequately protect their own forces or the indigenous population from attack. When unable to stop the attacks, Army units cannot establish the security that is essential to restore public utilities and perform those other tasks critical for Iraq to emerge as a normal country.[9]

As a partial remedy, the Quadrennial Defense Review directed that U.S. forces would fight the long war principally "by, with, and through others." Those who live in the neighborhood, speak the languages, and understand the cultures of the local people presumably can be more effective at identifying the enemy.[10] The recent "Awakening" councils and the emergence of the Concerned Local Citizens and Sons of Iraq lend support to this point of view.[11]

Against more traditional adversaries who employ regular military forces, the U.S. military has been dominant. The Taliban and its supporting militias, when they elected to stand and fight, faced destruction at the hands of the U.S.-led coalition forces. Iraq's army disappeared when confronted with the combined arms onslaught of U.S. joint forces. However, in disappearing, individual soldiers and leaders, operating as an irregular force, maintained their ability to attack U.S. forces and oppose U.S. forces' operations. Using irregular warfare tactics, they posed a threat much harder to find and defeat, and the information superiority advantage shifted from the United States to

---

[8] This is clearly true in SSTR operations and irregular warfare. This situation also emerged in major combat operations in Operation Iraqi Freedom (OIF), including Iraqi attacks against U.S. forces in urban areas and attacks by irregular forces (for example, the Fedayeen) during the advance on Baghdad.

[9] We must clearly distinguish between what Army units can do on their own, with network-enabled forces, and what Army units can do with significant help from indigenous actors. Here, we assess the organic capability of U.S. military forces, as made available to Army units at the lowest tactical levels. The recent "Awakening" councils and Sons of Iraq have also provided vital intelligence to coalition forces on the location and activities of insurgents in Iraq. The network can and should be designed to facilitate the receipt and use of this information.

[10] U.S. Department of Defense (2006).

[11] In fact, the information provided by these local groups is often credited with tipping the balance against insurgent groups in Iraq. If true, this argues that developing the human network in Iraq was a necessary condition for effective counterinsurgency operations.

local insurgents. Such a shift could happen because U.S. forces need far more information (for example, to identify and neutralize a few insurgents in a crowd of civilians) than insurgents need (for example, to find and kill a few easily recognized U.S. soldiers in a convoy on a frequently used roadway, especially if the insurgents do not try to avoid collateral damage).

A similar problem may emerge in future major combat and counterproliferation operations. Enemies could plan to hide conventional forces among civilian populations, making it difficult to discriminate combatants from noncombatants until there is direct contact. Past adversaries (notably Serbia) have also located their forces (such as air defenses) near religious sites and other "no-strike" locations. Future adversaries might protect other high-value capabilities—such as WMD, TBMs, and command and control (C2) nodes—through a combination of hiding them among civilian populations and moving them to evade destruction.

CHAPTER THREE

Tactical Information: What Commanders and Leaders Need to Know

This chapter examines the information that commanders and soldiers need to overcome the challenges presented by current and future conflicts. This includes conducting MCOs, SSTR operations, and irregular warfare operations. U.S. Army units dominated enemy regular forces in recent major combat operations but have struggled with insurgents and other irregular forces. This suggests that the network should be improved in ways that better enable successful SSTR and irregular warfare operations. Once it is known what information commanders need, the network can be adapted to help find that information.

Information Needed for Major Combat Operations

The Army's LandWarNet Office has described the information needs of soldiers in the field and has established a set of guidelines for meeting these needs.[1] Soldiers in the field today are faced with

- a complex battlefield environment
  - that places increasing demands on individual soldiers and junior leaders to make key battlefield decisions
  - that were once made by senior leaders

[1] Conversation with Michael Eixenberger, HQDA G-3/5/7, DAMO-LB Deputy Director, December 17, 2010, and United States Central Command Briefing, December 10, 2009, CENTCOM TF 2/3/6.

- complex coalition efforts that place additional burdens on tactical formations
  - to share common information with coalition partners
  - to collaborate to achieve desired battlefield effects
  - with a potentially large number of coalition parterns
  - that have varying degrees of technological capabilities.

Challenges that the LandWarNet Office faces include

- providing greater bandwidth
  - often to disadvantaged users
  - some of whom utilize non-U.S. equipment
- integrating voice and data networks to support ability to
  - develop and execute plans collaboratively
  - synchronize execution across all domains
  - monitor execution
  - assess effects
  - adapt operations on the move.

At the time of this analysis, the Vice Chief of Staff of the Army authored a "blue note" that summarizes his view of the key information that commanders and leaders need. These items of information were expressed as key questions for battle command,[2] summarized as follows:

- Where am I?
- Where are my [Joint] buddies?
- What am I doing?
- Where is the enemy?
- What is the enemy doing?
- Where is the enemy vulnerable or at risk?
- Where am I vulnerable or at risk?
- What should I be doing next?

[2] Handwritten note by General Richard A. Cody, Vice Chief of Staff, United States Army, shared with the authors at HQDA G-3/5/7, January 25, 2007, The Pentagon, Arlington Virginia.

- What are the potential implications of my next actions to deal with the assessed risk?

Where am I? It is of primary importance for all warfighters to know the position of Army, joint, and coalition forces. This awareness begins with knowing one's own position. It is vital that soldiers and leaders know their own positions in the context of terrain at all times for effective land navigation and maneuver. Commanders and leaders at every echelon also need to know where their subordinate soldiers and units are (this is a broader sense of the term "I"). Subordinate units may be spread out—beyond the ability of a parent unit to provide immediate support. Therefore, it is also useful—and arguably necessary—for units at every echelon to know the location of sister units, adjacent Army units, and other joint and friendly forces, as we explain next.

Where are my [joint] buddies? Warfighters need to be able to synchronize operations with other friendly forces. This begins with knowing the position of friendly forces and being able to identify who and what those friendly forces are to avoid fratricide and to incorporate them in tactical actions. For example, maneuver battalion and company commanders need to know which units to expect on their flanks or passing overhead. Commanders use this information to coordinate fires and maneuver to help avoid fratricide and achieve the desired battlefield effects. If friendly forces come under fire, this information may enable an adjacent unit to promptly provide reinforcement or relief. Finally, commanders responsible for an area of operation (AO) or a zone of action—*zone owners* in our parlance—may want to know who enters or crosses their zone. For example, this information can help battalion and company commanders coordinate operations with convoys (such as clearing areas of enemy forces ahead of a convoy or exploiting insurgent attacks as opportunities for attacking enemy forces once they expose themselves).

A deeper level of situational awareness would include unit type, identification number, and the frequencies and call signs used by their commanders to communicate. It might also be useful to include some information about the units' assigned missions (reconnaissance, logistics convoy, and so on) and current status (enemy sighted, troops in

contact, for example). (Much of this information is available today through the SLANT report[3] via Blue Force Tracker [BFT].)

Finally, units will need to know which coalition or host nation forces are operating nearby so that operations can be synchronized with them in much the same way as with U.S. forces.

What am I doing? Commanders need to know what Army, joint, and coalition forces are doing so that they can synchronize the operations of units that depend on each other or are likely to meet in some way. (This is a broad use of the term "I," and includes assigned, attached, and supporting units and those liable to be so directed.) Therefore, commanders need to know about combat forces patrolling, moving, or fighting adjacent to each other; convoys moving through battalion zones; and unmanned aerial vehicles (UAVs) and other aircraft patrolling in the vicinity of friendly forces so that they can make full use of these resources if the situation changes in some significant way.

Where is the enemy? The other side of situational awareness is the ability to detect, locate, identify, and target enemy forces before they have the opportunity to do the same to U.S. forces—and then to distribute this information widely among blue units. A necessary first step is projecting when and where the enemy might be found. Projections may be based on recent enemy behavior or on estimates of where the enemy may have the best opportunities to rest, refit, train, or plan and execute operations.[4] Knowledge of the enemy might be collected firsthand by the reconnaissance and surveillance efforts of each unit. The parent unit and other units in theater represent additional sources to locate enemy forces. All forms of human intelligence (HUMINT), and especially intelligence gathered in the regular course of soldier activities, will serve as an important source. Tips from local civilians may become the most important source in some situations (more on this topic in the next section).

---

[3] SLANT reports give the operational status of a unit, by its type of weapon system.

[4] RAND colleague Tom Sullivan has developed an analytic methodology to predict "hot spots" of future enemy activity. This technique, and similar techniques used by deployed Army units, can inform these projections.

What is the enemy doing? Unit intelligence personnel try to figure out what the enemy is doing, typically by making inferences based on the enemy's size, composition, disposition, and behavior. Additional impressions will come from the same people, units, and assets that found the enemy in the first place. Estimates of what the enemy appears to be doing will guide a commander's future actions. These estimates will also be used to plan the deployment of the limited intelligence, surveillance, and reconnaissance (ISR) assets available at echelons of battalion level and below. Assets might include unattended ground sensors, UAVs, helicopters, reconnaissance patrols, HUMINT, and the communication equipment to receive direct downlinks from Army or joint systems.

Where is the enemy vulnerable or at risk? An item of great interest is a running assessment of where an enemy might be vulnerable or at risk. Such an assessment is greatly aided by actually seeing enemy forces and knowing something about their location and activities. An enemy can greatly complicate this assessment if he can remain hidden (for example, by using complex terrain or employing camouflage and deception techniques) or can avoid presenting himself (for example, by using guerrilla tactics). In any event, U.S. and allied forces must anticipate where they might meet enemy forces and prepare alternative courses of action to turn those accidental encounters into opportunities to destroy the enemy.

Where am I vulnerable or at risk? The Army should expect the enemy to find and exploit weaknesses in Army, joint, and coalition forces. If the Army can discover the enemy's vulnerabilities first, it might deny him an opportunity to attack. Better still, U.S. forces might be able to effectively set traps for adversaries.

What should I be doing next? In warfighting contingencies, soldiers and leaders typically spend a great deal of time identifying the best ways to defeat the enemy. Presumably, much of this time is spent in a hierarchical fashion preplanning how subordinate units will accomplish their individual tasks as part of a larger operation. To take advantage of a networked force, courses of action also need to be developed to enable a unit to respond to emerging information provided from multiple places in the battlespace. Therefore, the Army will want

ground and air forces ready to quickly engage enemy forces where and when they appear.

What are the potential implications of my next actions to deal with the assessed risk? Enemy leaders will seek to take advantage of the actions that U.S. forces have taken, as well as the actions that U.S. commanders decide not to take. Clever adversaries will seek to exploit U.S. actions and decisions for political, military, and intelligence purposes. Units at the tactical edge may be able to use networks to provide faster reporting of events to higher headquarters, thus revealing the point of decision for the current engagement or suggesting how follow-on actions might exploit local successes and bring the operation to a successful conclusion on U.S. terms.

Information Needed for Security, Stabilization, and Reconstruction Operations

From an operational perspective, it is useful to think of SSTR operations as existing between the realms of major combat operations and irregular warfare. From the vantage point of conducting SSTR operations, Army officers should be able to sense whether they are achieving stability and security that will lead to the withdrawal of U.S. forces or whether the situation after an MCO is deteriorating and slipping toward irregular warfare. As a result, SSTR operations and irregular warfare receive a slightly different treatment here than they might in a canonical, doctrinal text.

During SSTR operations, the questions relating to combat remain important for dealing with any residual organized resistance, but they must be supplemented with other questions whose answers get to the heart of the tasks inherent in SSTR operations, including:

- Who are the local authorities and how capable and trustworthy are they?
- What enemy and criminal elements are operating in my area?
- What threat do they pose?
- What must I protect?

- What must I restore?
- Whom among the locals can I count on for help?

These are likely to be the most useful questions in SSTR operations because they refocus the tasks of battle command on the objectives of SSTR operations: providing security, restoring functioning governance and public services, and reestablishing the social contract between the population and the government (or interim government). Unfortunately, the battlefield intelligence systems, UAVs, and other tactical hardware that served well during major combat operations function less efficiently in providing answers to these questions.

Who are the local authorities and how capable and trustworthy are they? Tools not traditionally thought of as military must be deployed to find answers to these questions. Officers can consult local government records and newspapers, meet firsthand with the officials in question, inquire among nongovernmental organizations (NGOs) with long-term knowledge of the region, consult with academics and the diaspora community, or survey the public. Commanders need some standards against which they can assess the potential of local authorities to address the many challenges. For example, following Operation Iraqi Freedom, the Coalition Provisional Authority relied heavily on academic credentials and vetting within the Bush administration and got very uneven performance from the local officials they selected.[5]

What enemy and criminal elements are operating in my area? HUMINT and perhaps signals intelligence (SIGINT) might provide some useful intelligence about lingering resistance and criminal personalities, but to get their identities, capabilities, motives, numbers, and whereabouts, information from the (remaining) local police, from NGOs, and from neighborhood leaders is also probably needed. Commanders must differentiate between information about real enemy fighters or criminals and otherwise innocent individuals against whom Army sources have grudges. Commanders also must determine which actors pose a serious threat to U.S. forces' success in SSTR operations and which are merely a distraction or minor disruption of public order.

[5] See Allawi (2007).

To do so, Army units will need soldiers trained to read documents and visit Web sites published in the local language; they will also need the skills to aggregate the judgments of NGOs and local personalities to provide robust assessments of the threat posed by enemy combatants and criminals in the area.

What threat do they pose? On the specific question of threat, in addition to the sources already mentioned, soldiers might look for enemy literature, speeches, graffiti, and Web sites to ascertain the nature of the threat. Soldiers with the cognitive skills to assess these threats in the context of the country in question will be needed.

What must I protect? This is a key question in SSTR operations because security is the fulcrum for stabilization and reconstruction operations. If security improves, then stabilization and reconstruction initiatives can tip society in a positive direction, thereby enhancing the prospect for a return to normal life for the inhabitants and an expeditious return home for U.S. forces. If security deteriorates and society tips into irregular warfare (or worse), then the inhabitants face the prospects of intolerable living conditions and the potential collapse of their state, and U.S. forces face the prospect of extended deployments and nearly endless skirmishes with guerrilla fighters. Determining what the inhabitants value and what must be protected therefore becomes a key task. Public records, municipal plans, NGOs, and local officials represent key sources.

What must I restore? The answers to this question are critical to rebuilding the social contract in the country and establishing the legitimacy of the new government to rule. In addition to public records, NGOs, and public officials as sources of information, commanders may need new types of information, especially where public utilities are concerned. Questions include: What was the former output and demand? How do we assess current production capacity? The civil affairs community typically deploys soldiers with the skills to help answer such questions.

Whom among the locals can I count on for help? This question differs from "who is capable and trustworthy" because it also involves matters of inclination: Who will set aside their prejudices and preconceived notions and help the stricken society recover? For example,

soldiers need to understand: Will a particular Sunni officer set aside his prejudices to restore clean water to a Shia neighborhood? Or, will a Tamil find sympathy for a Shalalah government official and help him? Will a Kurd find common cause with an Arab? Understanding may require the kind of empathy that develops fully only from sustained interaction with the populations in question.

Information Needed for Irregular Warfare

The questions associated with battle command in irregular warfare are more complicated and diverse than the "where" questions of MCOs (Where am I? Where are my buddies?) or the "what" questions of SSTR operations (What must I protect? What must I restore?), because they combine "who," "what," and "how" questions:[6]

- Who is the enemy and what does he want?
- Can we dissuade the enemy (for example, reintegrate him into local politics)?
- What population is the enemy trying to influence and how do we insulate them?
- How do we identify the enemy?
- How do we locate the enemy?
- Who can help us?

Who is the enemy and what does he want? These questions may be answered in part through classic biographical intelligence, HUMINT, and exploitation of enemy Web sites. However, a more complete understanding of the enemy—identities, capabilities, motives, numbers, and dispositions—is possible only with the help of local authorities, regional experts, NGOs, and similar entities with a longer-term, more intimate understanding of the adversary. The Army therefore needs capabilities that can help soldiers and commanders

[6] These questions derive from Headquarters, U.S. Department of the Army (HQDA) (2006).

understand the sometimes-subtle importance of alien religious, cultural, and social concepts and the leverage they offer the enemy with respect to the local populace.

Can we dissuade the enemy? The answer to this question can help commanders understand the prospects (if any) for a compromise or concession-based solution. Compromises have been important historically. British concessions were key to ending the 1920 insurrection in Mesopotamia, the Malay emergency, and the Mau Mau insurrection in Kenya.[7] Commanders need help to appreciate the acuteness of the dispute, the prior attempts at reconciliation and reasons for their failure, and the fundamental nature of the dispute (for example, is it a zero-sum game and therefore impossible to resolve short of force-of-arms?). Public statements by all parties and the perspectives of officials, regional experts, NGOs, and similar observers might all serve as inputs. At the end of the day, the U.S. commander should emerge with a clear appreciation of whether a brokered solution of some sort is possible or whether the irregulars must first be destroyed.

What population is the enemy trying to influence and how do we insulate them? Irregular warfare tends to emphasize influencing a target population rather than closing with and destroying the adversary by fire and maneuver. The target population could be a minority embedded within a larger community (for example, Sunnis or Kurds in Iraq). Knowing their numbers, locations, social organization, and leadership will become important. Commanders must be able to mine local officials, enemy literature, Web sites, and NGOs to understand the stakes in the struggle. Commanders must also understand the measures available to insulate the targeted population from violence: Can their physical security be improved? Might they be resettled away from their tormentors?

How do we identify the enemy? How do we locate the enemy? These two questions are perhaps the most difficult. The answers may lie in some combination of informants, emblematics, biometrics, tagging/

[7] On Mesopotamia, see Jacobsen (1991, pp. 323–363), and Bell (1920). On the Mau Mau insurrection, see Hughes (1984), and Britain's Small Wars. See also Boddy-Evans (undated). For the Malayan emergency, see Clodfelter (1992), and "Malayan Emergency" (undated).

chipping strategies, or other methods that would allow U.S. forces to track suspects and correlate their presence with acts of violence. Commanders must determine which identification strategy is most likely to prove effective and which locating strategy is most likely to produce the desired results. For example, instrumenting with cameras a neighborhood full of irregular fighters and tagging the residents (such as with radio frequency identification chips in identity cards) may be feasible if the scale is manageable but may prove infeasible if an entire city of millions of residents is in open rebellion. Fundamentally, commanders need cognitive tools to help differentiate between the enemy and noncombatants and help separate the fighters from the peaceful populace.

Who will help us? The final battle command question for irregular warfare is concerned with potential sources of support for U.S. forces' efforts. Are there local forces with whom U.S.forces can collaborate, perhaps local officials? What are their identities, capabilities, motives, and numbers?

Summary

The Army's tactical information needs have traditionally been oriented toward making conventional warfare more efficient. Current and future commanders need to obtain similar kinds of information, but they will also require concepts specifically tailored for stability and irregular operations.

CHAPTER FOUR

Network-Enabled Operations

Various organizations and individuals within the Army are developing networks to provide the sorts of information described in Chapter Three. Some of these are formal programs of record; others are "soldier initiatives," sometimes begun by corps commanders and provided downward and at other times started by company-grade officers and enlisted soldiers and rapidly adopted by their peers. In this chapter, we broadly describe the networks in use or under development to enable tactical operations. We then describe how these networks are supposed to help and provide some metrics for their design, use, and assessment.

What Is the Network?

Before we describe our approach to addressing the questions in Chapter Three, we need to define the term *network* as we use it in this monograph.

The Army uses literally thousands of networks, especially when one counts all the local area networks at each echelon from theater Army, through corps and division, and then down to brigade, battalion, and company levels. These networks include those used by the operating forces for command and control, intelligence, maneuver, fires, and logistics as well as those used by the generating force at bases in the continental United States (CONUS) and abroad.

In 2004, the Army announced that LandWarNet would be the name for all Army networks and that it would combine the infostructure and services that process, store, and transport information.[1] The

[1] Boutelle (2004).

U.S. Army Training and Doctrine Command (TRADOC) provides a sweeping definition of LandWarNet:

> LandWarNet is the Army's contribution to the Global Information Grid (GIG) that consists of all globally interconnected, end-to-end set of Army information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand supporting warfighters, policy makers, and support personnel. It includes all Army (owned and leased) and leveraged DoD [U.S. Department of Defense]/Joint communications and computing systems and services, software (including applications), data security services, and other associated services. LandWarNet exists to enable the war-fight through Battle Command.[2]

We do not attempt in this monograph to assess the whole of LandWarNet. Such a comprehensive assessment was beyond the scope of this study. Instead, we examine the capabilities that the deployed portion of LandWarNet (hereafter referred to simply as "the network") provides to soldiers and leaders conducting operations. In that regard, we focus specifically on the network systems that carry Secret classified information: Secure Internet Protocol Router Net (SIPRNet), BFT and Force XXI Battle Command, Brigade and Below (FBCB2). We also discuss some network-enabled systems such as Command Post of the Future (CPOF). Most especially, we examine the capabilities that the network provides in four areas:[3]

- the physical components, including the radios, terminals, routers, landlines, etc., that constitute the network infrastructure and provide network connectivity
- the information environment, including the databases in which information is created, manipulated, and shared
- the cognitive area, which resides in the minds of soldiers and leaders and includes any sense-making tools they may have at

[2] TRADOC (2006a).

[3] Vane (2007). These areas closely compare with the domains as described by Alberts, Garstka, and Stein (1999).

their disposal that aid or enable situational awareness, situational understanding, decisionmaking, and planning
- the social area, which includes organizational relationships, collaboration, and the synchronization of actions and is found in doctrine, tactical standard operating procedures (SOPs), habits of mind, TTPs, and habitual associations between units, soldiers, or leaders.

When considering what is "in" the network, there is no clear dividing line that segregates sensors or databases as "outside." We consider all such elements if they are connected to the network to enable the operations of U.S. soldiers today.[4]

Finally, we present our analyses in terms of network-enabled operations. When describing the operations of its soldiers as aided by various material systems, including networks, the Army uses the term *network-enabled*.[5] Since the essence of our analysis is the degree to which Army networks are helping soldiers conduct operations, we use the term *network-enabled operations* throughout this monograph.[6]

---

[4] See HQDA (undated).

[5] For example, LandWarNet is defined as "the compilation of systems and applications, joined to form a *network-enabling* capability supporting the warfighter" (Boutelle, 2004) [emphasis added], or "LandWarNet is the means for Soldiers, leaders, and units, today and in the future, to conduct *information-enabled* joint warfighting and supporting operations" (Wallace, 2006) [emphasis added].

LTG Thomas F. Metz (2007) put his views on network-enabled battle command more emphatically: "Warfare is not 'network centric.' It is either 'people centric' or it has no centre at all," and "the true 'centre' of effective command and control (C2) remains the commander."

[6] The Army typically uses the terms *net-centric* or *network-centric operations* to describe how it is integrating hardware into concepts of operation (CONOPs). The hardware (or materiel) component of CONOPs has traditionally focused on platforms or weapons but now focuses increasingly on the network that ties them together. So the network is now at the center of the materiel systems incorporated into CONOPs.

How Is the Network Expected to Help?

If the network is to help address the most pressing tactical needs, it must develop in a way that allows Army units to identify, track, and destroy or neutralize its adversaries.[7] The Army needs to be able to collect and assess the kinds of information described in Chapter Three and distribute it to forces dispersed across a large battlespace. The Army has pinned its hopes on a very capable network to see and understand the enemy (before the enemy can see or understand U.S. troop movements), take action first, and finish the enemy decisively. The ideal network would help to provide the information needed by connecting soldiers and leaders vertically across echelons, horizontally across Army and joint units, and outwardly with allies, coalition partners, and host nation authorities and citizens. Once connected, networked units could then synchronize the operations of these dispersed elements to act as a coherent force.

Metrics for Building Networked and Synchronized Forces

In its future-oriented operational concepts and doctrine, the Army describes the contributions of its planned networks in terms of see first, understand first, act first, and finish decisively.[8] This "quality of firsts" has become ubiquitous in Army publications and serves as a "bumper sticker" expression of the Army's expectations for network performance.[9] Therefore, our research explores the degree to which the network delivers these capabilities.

This section describes the elements of see first, understand first, act first, and finish decisively in terms of the information necessary

---

[7] The Quadrennial Defense Review calls for this capability. See U.S. Department of Defense (2006).

[8] The see first, understand first, act first, finish decisively construct has become ubiquitous in Army CONOPs, briefings, and remarks by its top leaders. See Vane (2007) and Geren (2007).

[9] See HQDA (undated, 2003) and Office of the Secretary of Defense (2005).

for the different types of operations that we assessed in the prior section. Table 4.1 organizes the elements that we assessed in the preceding chapter for major combat, irregular warfare, and SSTR operations.

Table 4.1
Knowledge Components of See First, Understand First, Act First, and Finish Decisively for Different Types of Operations

Component	Major Combat Operations	Irregular Warfare	SSTR Operations
See first	Where am I? Where are my [joint] buddies? What am I doing? Where is the enemy? What is the enemy doing?	Where am I? Where are my [joint] buddies? What am I doing?	Where am I? Where are my [joint] buddies? What am I doing?
Understand first	Where is the enemy vulnerable? Where am I vulnerable?	Who is the enemy? What does he want? Can we dissuade him? What population is he trying to influence? How do we insulate them? Who can help us?	Who are local authorities? How capable and trustworthy are they? What enemy and criminal elements are operating in my area? What threat do they pose? Who among the locals can I count on for help?
Act first	What should I do next?	How do we identify the enemy? How do we locate the enemy?	What must I protect? What must I restore?
Finish decisively	What are potential effects of my next actions?	What are potential effects of my next actions?	What are potential effects of my next actions?

Seeing First

In our analyses, we categorize seeing first situations as those in which seeing is enough to understand and inform the needed action. In this context, seeing first includes all of the activities inherent in both broad and local situational awareness. For example, this includes the awareness of one's own position (including subordinate units and adjacent Army units), the position of joint forces (air, land, sea, and so on), and the current posture and activities of these forces. So seeing these forces includes becoming aware of their location, posture, and current activities and some confirmation of unit identity—most especially that these are friendly forces. This information is needed (or at least is highly valuable) for major combat operations, irregular warfare, and SSTR operations.

We argue that an enemy military force employing standard military weapons and tactics is easy to identify once detected. Therefore, seeing (by whatever visual, electronic, acoustic, or other means) the location and activities of an enemy force armed and operating in a conventional manner is enough to understand them and plan the appropriate action. Seeing thus satisfies the need to locate and discover the current activities of conventional enemy forces in major combat operations but is not necessarily revealing of enemy forces in irregular warfare or SSTR operations. (Nor does it cover the operations of unconventional or irregular forces in largely conventional campaigns; but it *does* cover enemy forces using largely conventional tactics or weapons in insurgencies or terrorist operations.) Issues associated with the problems of identifying and monitoring irregular or unconventional forces will therefore be addressed in the section below entitled "Understanding First."

The need for individual soldiers and leaders to see first can be met by actions that they take themselves (or are provided to them automatically) or by actions taken on their behalf by others. We refer to the first category of actions as *self-synchronization* and the second category as *electronic overwatch* in Chapter Eight of this monograph.

Understanding First

As we described in the previous section, understanding adds some level of analysis, organization, interpretation, and anticipation to what can

be seen. Understanding involves interpreting observations of the enemy for clues about his intentions, capabilities, and vulnerabilities.

In the case of major combat operations, understanding first includes an assessment of where the enemy is vulnerable and where U.S. forces and coalition partners may be vulnerable. For irregular warfare, a fair degree of analysis may be necessary to ascertain who the enemy is, given often-ambiguous surveillance and reconnaissance data. Analyses may also be needed to ascertain the enemy's immediate and long-term intent and to estimate the likelihood that he might be dissuaded from further fighting. Finally, understanding first includes identifying the population that enemy forces are attempting to influence, how U.S. forces might insulate that population, and who from the locale might be able to offer help.

In SSTR operations, a comprehensive understanding begins with identifying the local authorities, determining who is capable and trustworthy, and who can be counted on for help. Understanding first also includes identifying the enemy and criminal elements operating in the area and the level of threat that these elements pose.

Acting First

Acting first includes using information collected as described above to choose appropriate courses of action. For example, convoy planners might choose routes to avoid contact with an enemy given the latest information regarding recent enemy attacks. Convoy commanders might change their routes dynamically if enemy forces were suddenly spotted on the road ahead. Combat and security forces, on the other hand, may choose routes to block enemy forces or to seek contact on terms advantageous to U.S. or coalition forces.

Acting first might also involve tactical headquarters, for example, at the battalion or company levels, directing or approving lower-echelon units to employ fires and maneuvers to engage and destroy enemy forces. Some of these actions might involve U.S. ground forces engaging to preempt or defeat an enemy. Other actions might include authorizing aircraft to strike at emerging enemy ground forces, or preauthorizing areas as free-fire zones for joint and coalition forces.

In major combat operations, acting first begins with deciding on the preferred next steps in an operational plan. In irregular warfare, to act first may require developing alternative courses of action to identify and locate an enemy. These alternative courses of action will need to anticipate how an enemy might attempt to elude detection and identification. In SSTR operations, similar thought must be given to deciding which elements of a state or society are most important to protect or restore (for example, public infrastructure). Once again, alternative courses of action must anticipate the activities of civilians, criminal elements, and enemy forces.

Finishing Decisively

In major combat operations, finishing decisively includes killing or capturing enemy forces. The network plays a role here to the extent that it helps friendly forces close with and destroy the enemy. Such actions might include managing the dynamic targeting, surveillance, and tracking needed to maintain pressure on an enemy who is using movement, concealment, and deception in an attempt to escape. More broadly, the network plays a role in helping to identify the potential effects of a commander's actions and providing awareness of the location of blue forces to allow aggressive attack without fear of fratricide. These activities may require extensive inputs from entities outside the commander's headquarters. In these cases, the network will be vital for commanders to request and obtain the information that they need.

Evaluating Network Performance

The Army envisions that its networks will link all components of the warfighting enterprise to produce synergistic combat power. The Army proposes that networking geographically dispersed forces will lead to shared situational understanding of the battlespace that enables self-synchronization and enhances the effectiveness of joint and combined

operations.[10] Self-synchronization, in turn, is intended to accelerate command and, ultimately, military action.[11]

To assess these propositions, in the next few chapters we look at the experiences of soldiers in recent operations. In Chapter Five, we take a qualitative look at soldier experiences in recent operations by examining several case studies. In Chapter Six, we examine some quantitative measures from training exercises at the National Training Center and the Joint Readiness Training Center and some objective data from field operations. In Chapter Seven, we examine the results of an officer survey taken to assess network value.

---

[10] The current nature of irregular warfare in the Middle East raises the question of if and how network-centric warfare can marry both culturally dispersed and geographically dispersed forces.

[11] Alberts, Garstka, and Stein (1999).

CHAPTER FIVE

Military Utility of Network-Enabled Operations: Qualitative Assessment of Recent Case Studies

The case studies in this chapter serve to illustrate the performance of networks in actual operations. Based on narratives from after-action reports, these case studies summarize specific unit operations and thus indirectly describe the role of the network in the unit's activities. Wherever possible, we have tried to make the network's role explicit. The cases offer readers examples of unit operations and are intended to highlight network performance and to suggest where network enhancements might have made a difference in combat outcomes.

General Observations

As noted in Chapter Four, a principal motivation for networking Army units is to enhance their ability to see enemy forces first, understand the enemy's vulnerabilities before he can understand the vulnerabilities of U.S. forces, act before he can act, and then finish an action or engagement decisively. Just as important, the network is intended to allow friendly units to retain awareness of the positions and activities of each other. In this chapter, we seek to understand how well U.S. forces in fact can see, understand, act first, and finish decisively, and the consequences of not being able to do so. To this end, we explore several cases from recent operations in Iraq and Afghanistan. Our focus is on those units and situations in which networks are most needed: small units with limited organic capabilities, conducting operations alone at a distance from friendly forces, and against an enemy that can seize the tactical initiative at unexpected moments.

The goal of this analysis is to assess the degree to which forces at the tactical level are supported by their existing networks. Our hypothesis is that capable networks help units plan their operations, synchronize their efforts with those other forces, execute fires and maneuver with greater ease and flexibility, and dynamically replan their actions as the tactical situation changes. The cases that we have examined focus on units at the battalion, company, platoon, and squad levels—the echelons that, according to conventional wisdom, fall on the wrong side of the "digital divide" and typically lack the situational awareness and other network-enabled benefits available to higher-echelon forces.

These cases have received much attention and have been the subject of detailed studies. We do not repeat the whole of those detailed analyses here but instead use these cases to highlight the challenges that better networks might help units to overcome. In this analysis, we evaluate the ability of the units directly involved in the action, their higher headquarters, and adjacent units that could have affected the outcome of the action to see first, understand first, act first, and finish decisively.[1] We grade these capabilities for each case as red—for serious deficiency in the awareness and synchronization of those forces involved in or adjacent to action (including each unit's higher headquarters); yellow—for some positive capabilities and some significant issues negatively affecting outcome; and green—for forces aware and synchronized.

On the Advance: The Drive to Baghdad in Operation Iraqi Freedom

U.S. commanders have stated that they were never surprised at the operational and senior tactical levels of war during the advance to Baghdad in Operation Iraqi Freedom.[2] Commanders and staffs at the Army, corps, and division levels had unprecedented situational awareness and information regarding weather, terrain, and friendly and enemy forces.

---

[1] This desired state is codified in HQDA (2003).

[2] Wallace (2003); Fontenot (2004).

The confidence that senior ground combat commanders had in their networks allowed them to act with confidence while undertaking some bold actions with significant military risks.

First, the Army drive pitted two and a half divisions against a numerically superior enemy. The Iraqi forces under Saddam Hussein might have struck the long and exposed left flank of the U.S. forces numerous times during the advance. Likewise, significant regular forces might have hidden in the cities bypassed by the Army during the U.S. advance. But MG Buford Blount, commander of the 3rd Infantry Division (ID), was confident that he (and his superiors) would see enemy forces, and then destroy them, before they could close with his forces.[3] Later, General Blount approved the now-famous "Thunder Runs" because he trusted the ability of the Army networks to alert him to the presence of significant ground threats.

Similarly, then–MG James Mattis was confident that he could handle the risks posed by Iraqi forces to the 1st Marine Division on the eastern axis of advance. General Mattis stated that his networks enabled him to see and engage Republican Guard forces long before his relatively light forces closed with them.[4] This allowed the 1st Marine Expeditionary Force (MEF) to engage these heavy forces with artillery and airpower, reducing them to a few "dazed and dismounted" (and deserting) survivors. These survivors posed little threat to the advancing Marines. (However, enemy forces hiding in towns and cities did pose a significant threat, which we discuss next.)

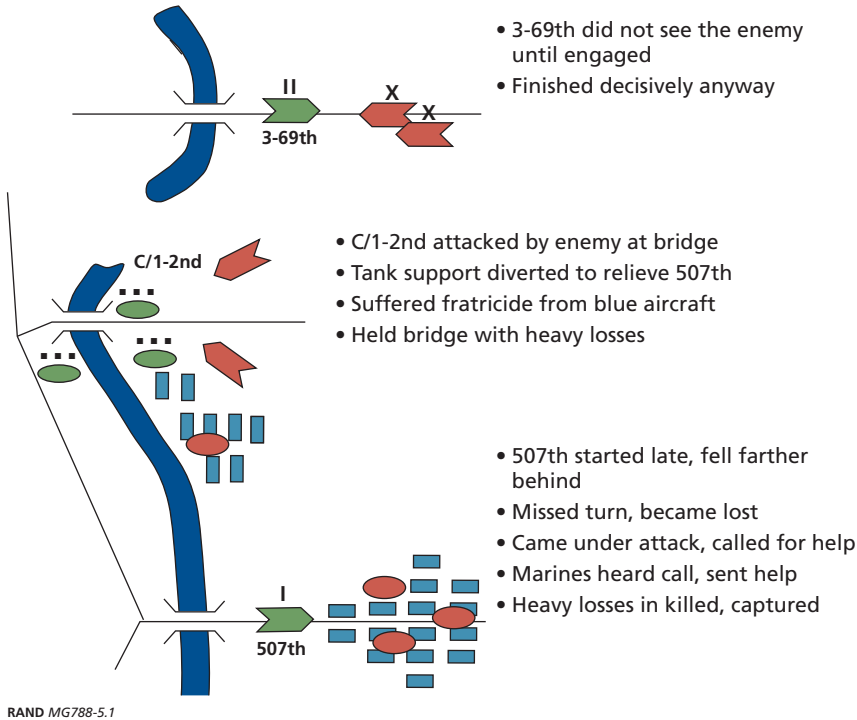
At the tactical level—especially at the battalion level and below—troops were often "moving to contact." Soldiers and Marines at these echelons did not have organic systems to find enemy forces in their path or approaching them—particularly when these enemies hid in urban areas. Sometimes, these troops were surprised by the enemy, as depicted in Figure 5.1, which illustrates separate events involving three units.

---

[3] MG Buford Blound (Ret.), 3rd Infantry Division Commander during OIF, interview with author, RAND Corporation, November 18, 2003.

[4] Mattis and Hoffman (2005).

Figure 5.1
Actions of the 3-69th Armor, C/1-2 Marines, and 507th Maintenance Company During Advance on Baghdad



The 507th Maintenance Company

The 507th had several problems, which an improved network might have helped them to overcome.[5] First, the 507th began its tactical movement without a feasible navigation plan. The commander decided to take a shortcut across open country rather than using the roads. This

[5] Subsequent analyses determined that the 507th Maintenance Company lacked some measure of the equipment and training needed to counterattack an enemy light-infantry unit. We do not dispute these findings, nor do we claim that a better network would have obviated the need for better training and equipping. Instead, our purpose is to determine how a better network might have improved the tactical situation for the 507th and the other units that we examine in this chapter.

shortcut was taken in the hope of saving some time and helping the 507th to catch up with other U.S. forces. Unfortunately, it took over five hours for the 507th to reach the road and the traffic control point outside Nasiriyah, thus rendering it farther behind and more isolated from its comrades.

At this point, the 507th mistakenly took the road into Nasiriyah rather than the road that bypassed the town. While driving through town, the little convoy attracted the attention of enemy irregular forces who rapidly deployed to snare the U.S. formation in an ambush. Eventually, the 507th realized that it had made a navigation mistake and began to turn around. The slow process of turning the heavy vehicles in the column presented an easy target for the enemy forces, which then sprang their ambush. Several vehicles managed to make it safely out of town and gave a Mayday call, which was received by the 2nd Marine Regiment (more on this unit next). Ultimately, a Marine armored unit was dispatched to the scene to rescue those soldiers who had not already made their way out of the town, been killed, or been taken prisoner.

Throughout this unfortunate engagement, the 507th's parent headquarters was apparently unable to track the progress of the 507th, determine that it had strayed from its route, or ascertain that it had come under attack. The higher headquarters also was not able to alert adjacent forces to come to the 507th's rescue. However, an adjacent unit headquarters did hear the radio voice traffic from the 507th and did organize a relief operation as described in the next section.

We assessed the network support to this engagement as:

- See first: The 507th did not see enemy forces until it had entered Nasiriyah. Adjacent units, the parent unit, and higher headquarters were not able to provide overwatch of the 507th.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Understand first: The 507th did not know what direction it was to take and did not understand that it was moving into a potential ambush. The parent unit and higher headquarters did not see that the 507th was alone and taking a wrong turn.

  - Assessment: red—serious deficiency in force awareness and synchronization
- Act first: The 507th was unable to find a route that allowed it to avoid the town and rejoin a convoy, was not able to avoid contact or make contact on advantageous terms, and was not able to (or did not) request immediate reinforcement or support. The parent unit, adjacent units, and higher headquarters were not able to see the 507th's predicament and push support to it (until the very end, when Task Force [TF] Tarawa heard the Mayday call over tactical radio).
  - Assessment: red—serious deficiency in force awareness and synchronization
- Finish decisively: The 507th was broken into pieces as it retreated, was engaged piecemeal by enemy forces, and suffered heavy casualties until elements of TF Tarawa arrived.
  - Assessment: red—serious deficiency in force awareness and synchronization.

Company C/1st Battalion, 2nd Marine Regiment

In a neighboring area, Company C/1st Battalion, 2nd Marine Regiment, was ordered to take the more distant of two bridges crossing the Tigris River near Nasiriyah. A tank platoon originally intended to accompany the Marine infantry was diverted to relieve the 507th Maintenance Company, which had come under heavy attack. Company B had attempted to maneuver north of Nasiriyah rather than go through the town, but its vehicles sank into the soft ground. Therefore, Company C riflemen in lightly armored amphibious vehicles attacked through Nasiriyah to reach the near side of the bridge. Along the way, they came under very heavy fire from Iraqi forces in the town.

Once clear of the town, the Marines established defensive positions on both ends of the bridge. They came under almost immediate attack from Iraqi infantry and mortar units and suffered significant casualties. To make matters worse, an Air Force A-10 called in to provide close air support (CAS) to the Marines mistook their amphibious vehicles for Iraqis' and fired on them, causing further casualties. Vehicles attempting to evacuate the wounded again came under fire as they

reentered Nasiriyah. Three of these six vehicles evacuating wounded were disabled in town, and their dismounted Marines began fighting from hasty positions while running low on ammunition. Ultimately, the Marines received reinforcements, held their positions at the bridge, and relieved their elements under fire in the town.

We assessed the network support to this engagement as:

- See first: Company C did not know that the route around town consisted of soft ground, which would represent an obstacle to maneuver. Company C did not see enemy forces either of the times it entered Nasiriyah until after it had come under attack. Higher headquarters did not know the posture of enemy forces.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Understand first: The aircraft sent to provide air support to Company C misidentified the company as an enemy unit and fired on it. Neither the Marine Corps nor Air Force higher headquarters was able to prevent the resulting fratricide. Marine Corps higher headquarters did not see Company C get ambushed the second time in Nasiriyah and was not able to help it avoid the ambush or provide immediate reinforcement or fire support. Neither did higher headquarters know that adjacent U.S. forces (that is, the 507th) were moving into an ambush and would need relief.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Act first: Company C was hit by enemy mortar fire before it could silence these mortars. The Company C casualty evacuation column came under vigorous attack, but was relieved some time after it had called for help. Similarly, the 507th was rescued after it had suffered significant casualties and some elements managed to escape and make contact with the Marines.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Finish decisively: The Marine force, including Company C, ultimately prevailed but suffered heavy casualties.

  - Assessment: yellow—significant issues negatively affecting outcome.

3rd Battalion, 69th Armored Regiment, at Objective Peach

The 3-69th had been ordered to seize and secure a bridge over the Euphrates River on the approach to Baghdad. After seizing the bridge, the 3-69th set up defensive positions on both sides. Army intelligence warned that scattered enemy infantry elements might attempt some form of attack at less than brigade strength. Instead, two Iraqi brigades reinforced with armor attacked the 3-69th. Although surprised, the 3-69th reacted quickly and decisively defeated the Iraqi armored and infantry forces.

We assessed the network support to this engagement as:

- See first: The 3-69th did not know that two brigades with significant numbers of armored tanks were in its vicinity and moving to contact.[6] The 3-69th commander had expected to be attacked by a smaller, lightly armed force and expressed surprise at coming under attack by a large armored force.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Understand first: A Joint Surveillance and Target Attack Radar System (JSTARS) aircraft overhead almost certainly saw the approaching force. Army and Air Force personnel on board would have logged the contact and transmitted the image to the ground via the Distributed Common Ground System (DCGS). However, such terminals would have existed at the Combined Force Land Component Command (CFLCC) and perhaps at V Corps Main HQ. No such terminals would have been available to V Corps Assault HQ (where then–LTG Wallace executed tactical com-

[6] It is possible that the 3-69th's parent brigade, division, corps, or Army HQ did see the enemy armored forces as they approached. However, this information never made it to the 3-69th.

mand), 3rd ID HQ, or brigade or battalion.[7] Also, no voice calls from either the JSTARS watch officers or CFLCC were received by the 3-69th. It is possible that neither the JSTARS nor CFLCC headquarters was aware that a friendly unit was directly in the path of advancing Iraqi forces.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Act first: The 3-69th lacked information to conduct fires or maneuver before coming under attack, so it did nothing until the Iraqis attacked.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Finish decisively: The 3-69th decisively engaged and destroyed the enemy. Although the available network did not provide the 3-69th with adequate awareness and synchronization from outside, the 3-69th defeated the enemy.
  - Assessment: green—the unit (at the battalion level) aware and synchronized.[8]

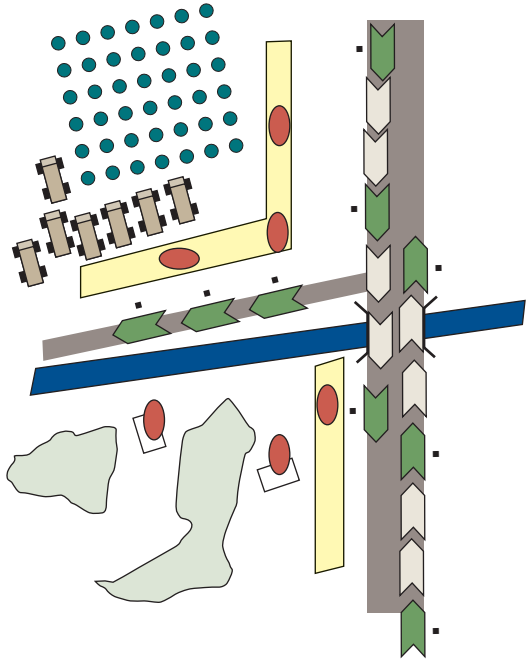
Convoys and Patrols: The 2nd Squadron, 4th Platoon of the Military Police Company, at the Palm Sunday Ambush

On Palm Sunday, 2005, two convoys were moving southeast of Baghdad in the vicinity of Salman Pak along Iraq Route 6, illustrated in Figure 5.2. One convoy was moving northeast (we refer to this at the "northbound" convoy) and the other southwest (we call this the "southbound" convoy). The convoys met as they crossed a bridge over an irrigation ditch and passed by an orchard and several buildings. At this

[7] Note that the DCGS-Army (DCGS-A) has been dramatically improved and expanded since this time. We discuss the DCGS-A further in the final section of this chapter.

[8] Here, we give a green rating to the 3-69th alone and rate its internal awareness and synchronization. It is a tribute to the 3-69th soldiers, and their excellent equipment, that they could overcome surprise and unfavorable force ratios to win so decisively. Although the results were desirable, we must also remember that the network above the battalion did not enable awareness and synchronization in the broader sense.

Figure 5.2
Actions of the 2/4/617th Military Police (MP) Company at the Palm Sunday Ambush



- Convoys fell into the ambush
- Convoys did not plan movement with MPs
  - MP squad happened by
- Enemy sprung the ambush as the convoys crossed
- Combination of MPs and convoy escorts defeated the enemy after an intense battle

NOTE: MP = military police.
RAND *MG788-5.2*

point, the convoys were attacked from enemy positions in the orchards and buildings and from ditches along the road.

The 2nd Squad, 4th Platoon, of the 617th Military Police Company came on the scene at this point. It had been patrolling the general vicinity of the ambush that day and decided to shadow the northbound convoy when it came into view. The squad was familiar with the orchard and farm buildings as a potential ambush position. As the convoy passed the orchard, the MPs recognized from the signs of smoke and evasive driving that the convoys were under attack.

The middle and rear portions of the convoys halted as their vehicles were taken under fire. The MPs raced alongside the convoys and drove onto an access road into the farm in an attempt to flank the insurgents. At this point, they noted seven vehicles parked with their

doors and trunks open—indicators suggesting an insurgent force of up to 50 fighters, a force far larger than they had anticipated. Although heavily outgunned, the MPs kept up a steady stream of fire to suppress and kill the insurgents. In addition, several gun trucks escorting the convoys maneuvered to provide supporting fires to the MPs. Several MPs then dismounted their vehicles and cleared the trenches on foot. Ultimately, the insurgents were either killed or driven off and the convoys (although suffering some losses) were able to regroup and resume their movement.

The MP Squad was ultimately able to decisively defeat the ambush with the support of several convoy escorts. (Several members of the MP Squad were later decorated for heroism.)

We assessed the network support to this engagement as:

- See first: Neither the 2/4/617th MP Squad nor the convoys saw enemy forces until they sprang their ambush. The MP Squad did not know the convoys' identity, when they were due into the area, what radio frequencies they were using, or their commanders' call signs. The convoys did not know that the MP Squad was in the vicinity and did not know that the farm and orchard were likely points for an ambush.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Understand first: At no point during the attack did any element within the MP Squad, convoy, or escorts have a complete picture of the battle. The 2/4/617th did not know the enemy's strength or disposition, and the convoy commanders were not sure what was going on outside their direct line of sight, which often extended no more than to the next vehicle.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Act first: Both the 2/4/617th and the convoy escorts were forced to recover from and respond to enemy attack. None of the MP or escort vehicles had more than sporadic communication with other vehicles, so they were not able to synchronize operations among their own elements or between the escorts and the MPs. The MP

Squad was able to request reinforcement and air support from its company headquarters, but both were many minutes away.
  - Assessment: red—serious deficiency in force awareness and synchronization
- Finish decisively: Through heroic action, the 2/4/617th and convoy escorts drove off or killed the insurgents.[9] Their success was driven by personal initiative and bravery and by the soldiers in individual vehicles moving in response to the sights and sounds of battle rather than by using a network to organize a response. On the positive side, the BFT system in the MP vehicles allowed the MP squad leader to broadcast his position to his higher headquarters (and offered some ability to send text messages to parent and adjacent units).
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting the outcome.

Army Combat Outpost: Defense, Overwatch, and Relief

The 1st Battalion, 24th Infantry Regiment (Stryker) was given the task of providing security to a large portion of Mosul during the second battle of Falloujah. At the time, enemy insurgents were increasing their presence in Mosul and posed a heightened threat to coalition forces. As part of its effort to increase security, the 1-24th decided to establish combat outposts in existing buildings at strategic locations in its AO. Manning these combat outposts would stretch the 1-24th's manpower, however, because the battalion also was obliged to participate in the defense of a forward operating base and had to continue its regular street patrols in Mosul.

Army intelligence had indications that insurgents were constructing vehicle-borne improvised explosive devices (VBIEDs) for possible use against these outposts. Therefore, the 1-24th decided to strengthen

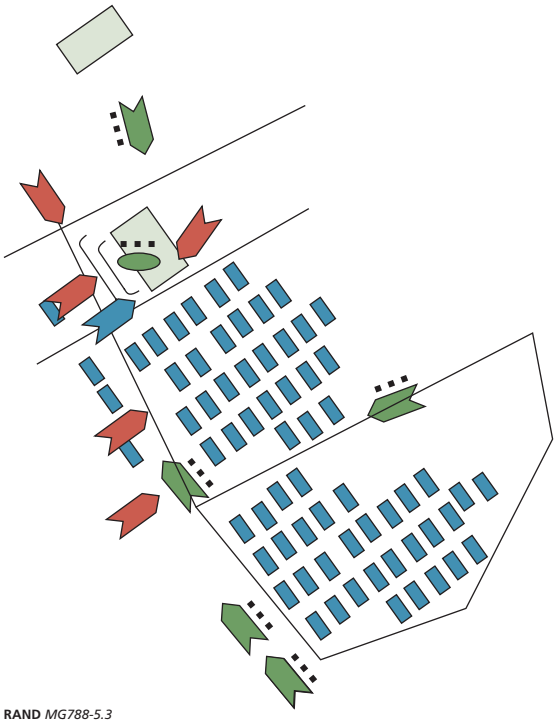
[9] The heroic actions of the 2/4/617th and the valor of soldiers from the convoy escort were sufficient to overcome tactical surprise and numerically superior enemy forces. However, losses were sustained and it would have been much better for these soldiers to have had a network able to help them avoid the grave situation in which they found themselves.

the fortifications of its combat outposts. One combat outpost (Tampa) was manned by 2nd Platoon, Company C.

The insurgents struck the 2/C/1-24th's outpost as predicted, using a VBIED to attempt to breach the fortifications (Figure 5.3). The large truck bomb failed to breach the newly strengthened defenses but did stun and wound platoon elements stationed in Stryker vehicles outside the outpost, killing and wounding soldiers in the outpost building. Following the blast from the VBIED, the insurgents launched their assault on foot using mortars and rocket-propelled grenades (RPGs).

As the U.S. platoon fought back, it alerted its company and battalion headquarters that it was under attack. Coincidentally, both the company and battalion headquarters elements were conducting patrols at that moment along with other elements from Company C and the

Figure 5.3
Actions of the 1-24th Infantry Battalion (Stryker) in Mosul



- 1-24th had intelligence indications of attack preparations
  - Reinforced platoon outposts
- Surveillance did not spot the attack
- Enemy attacked with truck bomb followed by assault on outpost
- Secondary ambush on relief forces
- U.S. forces prevailed, with losses

RAND *MG788-5.3*

1-24th HQ Platoon. These elements turned to provide reinforcements for the 2nd Platoon. At the same time, 3rd Platoon of Company C moved to block a potential insurgent escape route.

The insurgent forces had anticipated a movement to relieve the 2nd Platoon outpost and had placed additional improvised explosive devices (IEDs) on the outbound route that the 1-24th's patrols had taken a short time earlier. As the relief forces returned along those same routes, they were struck by this second IED attack. Several Stryker vehicles were damaged or immobilized, but the remainder continued on to relieve 2/C. Ultimately, the insurgents were killed, captured, or driven off.

We assessed the network support to this engagement as:

- See first: The 1-24th HQ did receive some intelligence that prompted it to reinforce the outpost. However, the 1-24th did not see the truck bomb before it detonated, did not see enemy ground forces until they had attacked the outpost, and did not see the second ambush before the attack on the relief column.
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting the outcome
- Understand first: The 1-24th Battalion HQ, Company C HQs, and other platoon outposts received an immediate voice alert from 2nd Platoon, Company C, that an attack was in progress. However, 2nd Platoon stopped transmitting once the heavy fighting started. Since the platoon members were in the building and had left their damaged vehicles, they did not provide further information to headquarters or relief forces. On the other hand, the entire battalion was able to monitor the progress of the relief column over the Strykers' digital communication devices.
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting the outcome
- Act first: Enemy forces acted first by prosecuting a series of attacks. The 1-24th Battalion HQ and Company C HQ responded soon after by altering their course to relieve Combat Outpost Tampa. Both battalion and company commanders were able to coordi-

nate maneuver and fires while moving toward Combat Outpost Tampa.
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting the outcome
- Finish decisively: The 1-24th decisively engaged the enemy and killed, captured, or drove off the insurgents. The battalion coordinated fires with several reinforcing platoons and multiple CAS sorties.
  - Assessment: green—force aware and synchronized.

Combat Reconnaissance: 1-3rd Special Forces Group at Syahcow

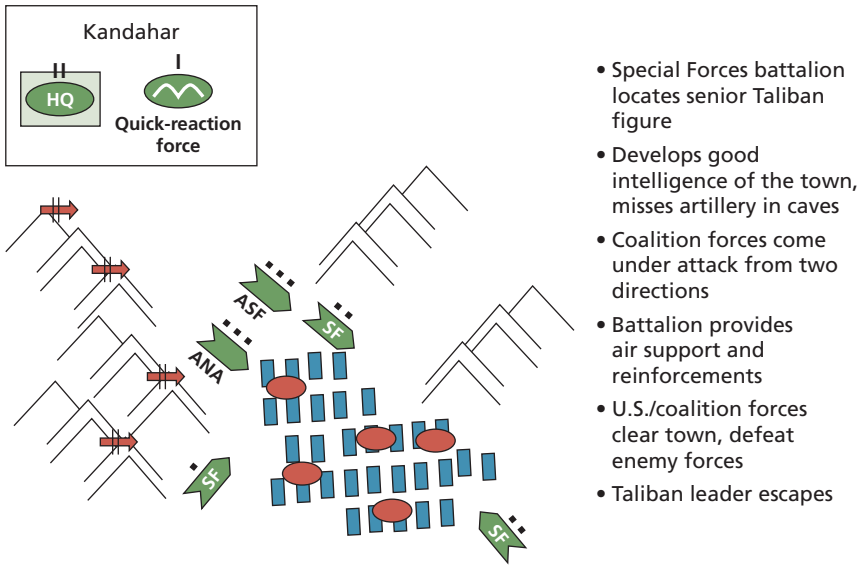
The 1st Battalion, 3rd Special Forces Group (SFG), had received intelligence that a senior Taliban official and a contingent of his followers were hiding in Syahcow, Afghanistan (see Figure 5.4). The 1st Battalion leaders decided to conduct a combat reconnaissance into Syahcow to search for Taliban forces and to kill or capture their leaders.

To that end, a combined force of Afghan National Army, Afghan Security Forces, and Army Special Forces Operational Detachment–Alpha (ODA) (ODA 324, with part of ODA 323) moved into position around the town. As the coalition forces took their places, Taliban fighters in Syahcow detected their arrival and some tried to flee. The subsequent pursuit alerted Taliban heavy weapons positions hidden in caves overlooking Syahcow. These weapons positions had escaped earlier detection by coalition forces.

At this point, much of the coalition force was in the uncomfortable position of taking fire from hostile forces behind and in front of them. It might have been possible to withdraw, but one element was in a particularly exposed position without a covered escape route. Worse still, withdrawal would have meant abandoning the mission of taking the Taliban leader.

Instead, the coalition force decided to request fire support and reinforcement from 1st Battalion HQ. Help came quickly in the form

Figure 5.4
Actions of the 1-3rd SFG at Syahcow



NOTE: ASF = Afghan Security Forces; ANA = Afghan National Army.
RAND *MG788-5.4*

of air support to suppress heavy fires from the Taliban-occupied caves. These air strikes were coordinated by Special Forces elements on the ground. Once the Taliban positions in the caves were destroyed or suppressed, the 1st Battalion landed a quick-reaction force (QRF) composed of an infantry company from the 82nd Airborne Division. The paratroopers, Special Forces, and Afghan forces then assaulted and seized the town. Unfortunately, the Taliban leader managed to elude capture (although he was killed in a subsequent encounter).

We assessed the network support to this engagement as:

- See first: The 1-3rd SFG saw the enemy in Syahcow and received early intelligence regarding the presence of enemy forces and leaders. However, the 1-3rd SFG but did not see enemy heavy weapons positions in caves overlooking village.
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting the outcome

- Understand first: The ODA on the ground was able to quickly grasp the situation and ask for help. The 1-3rd SFG HQ providing overwatch anticipated the potential need for reinforcements and fires support and so had placed a QRF and CAS aircraft on alert. When the request for support came back, the 1-3rd SFG understood the need to act quickly.
  - Assessment: green—force aware and synchronized
- Act first: ODA on the ground acted to maintain positions around Syahcow and 1-3rd SFG HQ ordered QRF to deploy and CAS sorties. Combined actions enabled ODA and 1-3rd SFG to regain the initiative.
  - Assessment: green—force aware and synchronized
- Finish decisively: The ODA, with QRF, CAS, and other reinforcements from 1-3rd SFG, silenced heavy weapons and cleared the village of insurgents. However, the Taliban leader escaped.
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting the outcome.

Counterambush: Manned-Unmanned Aircraft Teaming with Ground Forces

Over the past four years, U.S., Iraqi, and coalition forces have been subjected to frequent attack by insurgents, terrorists, and other anti-Iraqi forces (AIF). The AIF have conducted ambushes, launched indirect-fire attacks with rockets and mortars, and have used IEDs. These devices have been hidden alongside roadways, concealed in parked vehicles (VBIEDs), or used in suicide attacks (suicide vehicle-borne IEDs).

Great efforts have been made to neutralize these threats. The whole range of U.S. capabilities has been employed in various ways, including combinations of manned aircraft, unmanned aircraft systems (UASs), and ground forces. It is too early to determine which operating concepts will ultimately prove to be the most successful or whether these threats can ever be eliminated.

However, we can make some useful observations from some operations that have been successful. We have received reports of suc-

cessful manned-unmanned teams. Frequently, these operations have been part of Task Force Observe, Detect, Identify, and Neutralize—better known as TF ODIN. Other successful operations have been less formal—combining the operations of UAVs, ground forces, command posts, and sometimes manned aircraft to find and defeat insurgent forces.

We have also received reports that some operations involving UASs have failed or have not been able to exploit an opportunity to target insurgents. These missed opportunities have been attributed to a lack of synchronization between the UAS and the ground forces responsible for an area of operations. In some cases, the UAS has been controlled by a different unit or service and may have been engaged in a mission without previously synchronizing operations with the unit that controls a particular area of operations. Unfortunately, little hard evidence and few complete data are available to adequately describe the nature or cause of these failures. Therefore, we can note only that some opportunities appear to have been missed—this is probably inevitable, but we believe that it should spur the Army, its sister services, and the DoD to work harder to expand on those concepts that seem to be succeeding.

Therefore, we relate in the next few paragraphs several incidents in which combinations of air and ground forces succeeded in countering attacks on U.S. forces. We chose unclassified examples of successfully combining the elements of unmanned aircraft with sensor systems, a ground command post, and other warfighters in the air and on the ground.

1-24th: Shadow UAS, Strykers, and Joint Coordination Center

Some time after its operations at Combat Outpost Tampa, the 1-24th was alerted by the Joint Coordination Center that a VBIED had been placed in its area of operations. A Tactical HUMINT Team source then provided a detailed description of the vehicle and its exact location. In response to this information, the 1-24th moved a Shadow UAS to observe the suspected VBIED and its immediate surroundings. After confirming the suspected vehicle at the location as described, a Stryker Platoon was maneuvered to cordon off the area. An Explo-

sive Ordnance Disposal Team with robotic vehicles then "reduced" the VBIED, which contained 12 155mm artillery shells and a remote initiation system.[10]

TF 3-29th: F-15Es, Predator UAS, 101st Airborne (Air Assault), and the Balad Air Base Joint Defense Operations Center

Using a variety of fixed sensors and surveillance equipment (such as counterbattery radar), the Balad Air Base Joint Defense Operations Center (JDOC) detected mortars being fired at the base. The JDOC directed two F-15Es of the 379th Air Expeditionary Wing, on a close air support mission in the vicinity of Balad, to the point of origin. The F-15Es spotted a vehicle and three passengers fleeing the scene and followed the vehicles to a house. Meanwhile, a Predator was tasked to maintain surveillance and a quick-reaction force from TF 3-29th, 101st Airborne Division (Air Assault), was dispatched to perform a cordon-and-search operation. Ultimately, three suspects were detained, and evidence was collected implicating them in firing the mortar.

Scouts, Hunters, and the Brigade Tactical Operations Center

On September 1, 2007, U.S. Army scouts detected insurgents placing an IED near a roadway 180 miles northwest of Baghdad.[11] The scouts contacted their brigade Tactical Operations Center (TOC), which then tasked a Hunter UAS operating nearby. With the scouts' eyes on target, and the brigade TOC approving an attack on the target, the Hunter attacked and killed the insurgents with a laser-guided bomb.

5-73rd: Helicopters, Warrior UAS, and Brigade HQ

A helicopter operating with the 5-73rd cavalry (attached to the 3rd Brigade Combat Team [BCT], 82nd Airborne Division) spotted what appeared to be a squad of anti-Iraqi forces walking along a ditch often used by insurgents. When the group heard the helicopter overhead, they dispersed and hid.

---

[10] *Reduced* is the term used in the after-action report. We believe that the device was detonated safely.

[11] Osborne (2007).

The brigade headquarters then moved a UAS to continue surveillance of the area silently while the helicopter withdrew. Soon after the suspected insurgents could no longer hear the helicopter, they regrouped and began to emplace IEDs in a roadway, not knowing that they remained under the watchful eyes of the UAS. Once the brigade headquarters determined that the insurgents were a valid target under the rules of engagement, the helicopter was called back to prosecute an attack.

The helicopter subsequently attacked the insurgent squad, with two confirmed kills and some additional insurgents assessed to be killed or wounded.

Task Force ODIN

TF ODIN is an aviation task force organized to conduct reconnaissance, surveillance, and target acquisition (RSTA) operations to help combat the use of IEDs in Iraq.

Its purpose is to shorten the time between the detection of a target and the response by air or ground maneuver units. To do so, TF ODIN integrates planning, sensor cueing, and communications with aerial sensors, C2 systems, and other aviation and ground ISR systems. TF ODIN was organized at Fort Hood, Texas, and first deployed in October 2006.[12]

In February 2007, TF ODIN was organized into two companies and placed under the control of the 25th Combat Aviation Brigade (CAB). Alpha Company was organized to employ the Warrior Alpha Unmanned Aircraft System.[13] Warrior Alpha is an extended-range, multipurpose UAS equipped to employ electro-optical/infrared or synthetic aperture radar payloads and has a laser rangefinder designator and laser target marker. Bravo Company was organized from Reserve Component units equipped with C-12 airplanes outfitted as either aerial reconnaissance multisensor or medium-altitude reconnaissance and surveillance system RSTA platforms. Bravo Company is also equipped with Constant Hawk, which provides

[12] Campbell (2007).

[13] Wolf (2007).

forensic backtracking to determine the origins of attacks, and Highlighter, which identifies changes over time in terrain beneath a selected route of flight.

TF ODIN has developed TTPs to team these manned and unmanned RSTA assets with the CAB's rotary-wing platforms and supported ground units. Analysts onboard the manned sensor platforms transmit real-time imagery to maneuver units on the ground. They can also provide a sensor-to-shooter link by detecting and designating targets for CAB assets and the supported ground forces. In addition, TF ODIN can provide early IED warning for approaching coalition convoys.

This manned-unmanned teaming of Army aviation assets allows the ISR assets to observe, detect, and identify enemy forces while remaining out of sight and hearing range of the enemy. The rotary-wing aircraft can then engage from standoff ranges, retaining the element of surprise and reducing the threat to the manned platforms. As of January 2008, TF ODIN has killed 2,400 bomb-planters and captured 141 more.[14]

For the manned-unmanned teams examined in these cases, we assessed the network support to the engagements as:[15]

- See first: In the cases assessed, UASs, helicopters, and ground sensors were successfully used to spot insurgents on the move or conducting hostile acts. In some cases, the insurgents were spotted before they could spring an attack. In other cases studied, insurgents were caught in a violent act or while fleeing from the scene of an attack.
  - Assessment: green—forces aware and synchronized
- Understand first: Air vehicles and operation centers on the ground saw insurgents gather, act, or disperse and then handed target tracking and acquisition off to UASs and ground forces and granted permission for attack.

[14] Shachtman (2008).

[15] Note that these are the successful cases. We would strongly encourage the Army, the other services, and the DoD to also assess cases that did not yield positive results.

  - Assessment: green—forces aware and synchronized
- Act first: Helicopters or ground forces engaged insurgents who had been acquired and targeted by UASs.
  - Assessment: green—forces aware and synchronized
- Finish decisively: Some insurgents were killed and captured. However, some managed to escape, suggesting that the means to identify, track, and maneuver forces to destroy them requires additional improvement. This improvement appears to be under way, capitalizing on intelligence advances enabled by DCGS-A (described next) and operational advances embodied in TF ODIN.
  - Assessment: yellow—some awareness and synchronization, with some significant issues negatively affecting outcome.

DCGS-A, the "Flat Network," and Intelligence Support to BCTs and Below

In the course of collecting these case studies, we were given some new information from two officers recently rotating from units in Iraq and Afghanistan.[16] This new information concerned the need for "actionable intelligence" and an Army program under way to help deliver that intelligence to tactical commanders through a "flat network." That program, the network-enabled DCGS-A, has already led to some battlefield successes, so we chose to discuss the program here. Because some details of specific cases are sensitive or classified, we use only those operational comments provided in unclassified documents.

Timely and actionable intelligence is vital for successful operations, particularly against adaptive, irregular enemies. The Army defines actionable intelligence as that which "provides Commanders and Soldiers a high level of shared situational understanding, delivered with the speed, accuracy, and timeliness needed to conduct successful operations."[17] Up until this time, many ISR data have been available only to higher echelons (for example, at the theater Army or corps

[16] Discussions with LTC Gary W. Johnston and LTC David W. Morrison at RAND Corporation, Arlington, Va., March 20, 2008.

[17] Executive Office of the Headquarters Staff Group (2006).

level) from specific ISR ground stations (an arrangement sometimes referred to as a "stovepipe"). Information provided in this manner has often been criticized as not relevant on an operational time scale. The Army has begun a number of initiatives to provide actionable intelligence by making the network "flatter," that is, available across the Army at the brigade and battalion levels. Central to these efforts is the DCGS-A and the related Joint Intelligence Operating Capability–Iraq (JIOC-I).

The DCGS-A is designed to provide advanced networking, sensor connectivity, cross-cueing, data-sharing and processing, and targeting information to joint commanders at the tactical level. As a result of lessons learned in Iraq and Afghanistan, the Army completed expansion of DCGS-A fielding across the force down to battalion level in 2010 with further disposition available from the battalion- to company-level intelligence support teams. These capabilities are intended to provide commanders with a common view and understanding of the battlefield and timely access to any relevant ISR data. It is hoped that the DCGS-A will accelerate the decision-action cycle by providing situational understanding through a common operational picture (COP) tailored to the force, mission, and situation. Combined with other battlefield functional area capabilities, this is intended to enable unified action between Army commanders and joint warfighters through a common situational understanding of friendly forces, enemy forces, and the environment. It is also intended to help commanders understand the consequences as each interacts.[18]

The DCGS-A is the Army's LandISRNet foundation layer for LandWarNet. It is a network-enabled intelligence architecture that unifies sensor processing, analysis, exploitation, and visualization and interfaces tactical echelons with National/Joint intelligence data and applications. It is based on an evolution of Joint Intelligence Operations Center-Iraq (JIOC-I), which was conceived in 2004 to flatten the former hierarchical data networks into an integrated data repository enabling soldiers at every level with SIPR network access to search, retrieve, and visualize data without delay and filtration at successive

[18] U.S. Department of the Army, Procurement Programs (2007).

echelons.[19] Interim DCGS-A systems were fielded to corps level in Iraq in 2004 and to division level in Afghanistan in 2005 and were subsequently fielded down to battalion level across the Total Force by the end of 2010. In 2011, a more evolved DCGS-A with advanced analytics intended to improve the "Understand First" and "Act First" knowledge components of irregular warfare and SSTR operations was deployed to Afghanistan, and the Army will continue this evolution across the entire DCGS-A program.[20]

Currently, more than 200 data sources are available to analysts using DCGS-A and the number continues to grow, enabling unprecedented information-sharing. These data sources have been networked to function as "fusion brains"—repositories of data pertinent to a region, from which operators may draw actionable intelligence and to which operators and analysts may add raw or exploited data. (Note, though, that the exploitation and fusion tasks often are the most difficult challenges. Left undone, the power of the fusion brain may be diminished.) The power of the network-enabled DCGS-A Fusion Brains began with Iraq in 2004, Afghanistan in 2005, Horn of Africa in 2006, and the 513th Military Intelligence Brigade, which supports predeploying units in the Central Command (USCENTCOM) area of responsibility. The Fusion Brains were extended to other regional areas of responsibility such as European Command, Southern Command, Pacific Command, and Northern Command and will continue to evolve with enhanced capabilities as the LandISRNet foundation layer that supports ISR activities from deployed tactical formations and garrison overwatch. Later in this document, the study describes the use of formal and informal information capabilities by tactical users. Informal capabilities include capabilities such as mIRC Chat, Google Earth, and Soldier blogs. It is important to note that one of the Army's lessons learned from OIF/OEF include the ability to migrate user defined information capabilities into programs of record for use across the Force. To that end, programs of record including but not limited to

[19] Dubbed JIOC-I in 2003, the Army transitioned JIOC-I into the DCGS-A program of record in June 2006.

[20] Tactical units must have SIPRNet connections to these sites to access the information.

DCGS-A continue to evaluate and incorporate user-defined capabilities into its program. Google Earth and mIRC Chat clients have been included as part of the DCGS-A software baseline for several years.[21]

The information-sharing and analytic capabilities available through DCGS-A have led to the discovery of IED/weapons caches, insurgent safehouses, high-value targets, and threat cells. Division intelligence staff officers have praised the resulting capabilities; for example: "What previously took 20 hours of correlation, fusing, and plotting by hand now takes 10 minutes. Now we can fight the enemy, not the information."[22]

One final point is that intelligence support at the brigade level and below has been noted as a key enabler in recent operations to find, identify, and kill or capture insurgents in Iraq and Afghanistan. Interviews with recently returned brigades (including the 1st Brigade, 1st Cavalry Division, and the Combined Joint Task Force 82 in Afghanistan) indicate that the Human Terrain Teams, Cryptologic Support Teams, Military Intelligence Support Teams, and others have greatly increased the ability of brigade commanders to mount successful operations.

Summary Observations

Table 5.1 summarizes the observations from the cases described above. As equipped, some of the units in the cases that we examined had significant shortfalls in their ability to see friendly and enemy forces, to understand what those forces were doing, and to use that information to guide decisive action. However, two units had significantly better network capabilities: the 1-24th Stryker Battalion and the 1-3rd SFG. The Stryker units benefit from having the latest communication suites provided to conventional forces, and Special Forces typically emphasize command, control, and communication equipment and training to a greater degree than do most conventional units.

---

[21] The mIRC Chat capability will evolve based on theater requirements and DoD policy to migrate to a standards-based solution (e.g., Extensible Messaging and Presence Protocol.

[22] Guitard (2007).

Table 5.1
Summary of Unit Awareness and Synchronization in Historical Cases

	Unit						
Component	507th	C/1-2nd	3-69th	2/4/ 617th MP	2/C/ 1-24th Stryker	1-3rd SFG	Manned/ UAS Teams
See first							
Understand first							
Act first							
Finish decisively							

Also notable is the degree to which aircraft (both manned and unmanned), ground forces, and operations centers were able to conduct coordinated actions. This coordination was aided in some cases by the fact that the battle management function was conducted by operations centers at fixed sites and was endowed with the communication and C2 systems expected at such locations. Presumably, this same air-command post-ground coordination from mobile command posts will prove to be more difficult.

CHAPTER SIX

Military Utility of Network-Enabled Operations: Quantitative Assessment of Training and Operational Experiences

In this chapter, we present a quantitative examination of how well the network enables Army units to see first, understand first, act first, and finish decisively. For this analysis, we examined the Combined Information Data Network Exchange (CIDNE) and FusionNet databases to assess unit performance in Iraq. Together, these databases provided us with detailed information on unit activities and incidents, including engagements with the enemy from July 2004 through April 2007.

We hypothesized that, as the theater network matured and units became more adroit at exploiting it, we should be able to see the network's tactical benefits. Specifically, we expected that, over time, episodes of fratricide would decrease and units would become more skilled in discovering improvised explosive devices. Therefore, the ratio of IEDs discovered to those that detonate should shift in favor of the United States. Furthermore, the ratio of friendly to enemy-initiated incidents should shift in favor of the United States as U.S. troops exploited the network to get a better understanding of their area of operations and the enemy combatants operating therein.[1]

We also had limited amounts of training data that were collected from units exercising at the National Training Center at Fort Irwin, California, and at the Joint Readiness Training Center at Fort Polk, Louisiana. Our hypothesis was that a natural experiment lurked in

[1] However, we also note that this is a two-sided competition and that the United States should (and does) expect the enemy to also improve his effectiveness. Our hypothesis is that if U.S. forces achieve better network effectiveness, U.S. combat effectiveness will therefore increase faster than the adversary's.

the observer/controller scorecards that would allow us to see how a recent, network-enabled unit performed relative to an earlier, less-well-equipped unit of similar organization conducting similar training. We expected to be able to perform a similar time-series experiment by mining the Iraqi theater data to identify early-deployed units and, later, more network-endowed units that patrolled the same area of operations and to compare their relative performances.

Trends from Iraq

The results drawn from the CIDNE database are classified and are will be reported separately in forthcoming work. In this monograph, we refer to the March 2008 report to Congress, *Measuring Stability and Security in Iraq*, and other unclassified sources as noted.[2]

In brief, events in Iraq did not support our expectations about improvements in unit performance over time. Fratricide incidents seemed to vary with the intensity of U.S. and coalition operations.[3] Also, the proportion of IEDs found and cleared compared with the number detonated remained reasonably constant; the totals in each category increased as the enemy succeeded in deploying more of these weapons through the summer of 2007. Finally, the ratio of friendly to enemy-initiated incidents did not shift in favor of the United States and its partners through mid-2007.[4]

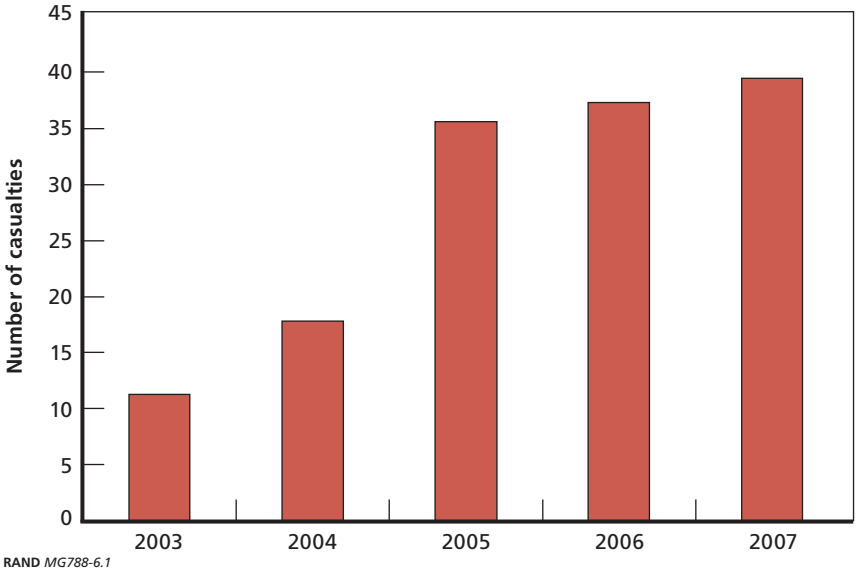
Indeed, despite all U.S. efforts, U.S. casualties from IEDs continued to mount through mid-2007, as Figure 6.1 illustrates. There is some evidence that anti-Iraqi forces increased the effectiveness of their

[2] *Measuring Stability and Security in Iraq* (2008).

[3] This information is based on unclassified data presented in a III Corps Safety Council briefing, March 30, 2006.

[4] See Bobby Ghosh, "The Enemy's New Tools in Iraq," *Time*, June 25, 2007.

Figure 6.1
Average U.S. Casualties per Month from IEDs, 2003–2007



attacks by using larger amounts of explosives in their IEDs and by using more sophisticated weapons, such as explosively formed projectiles.[5]

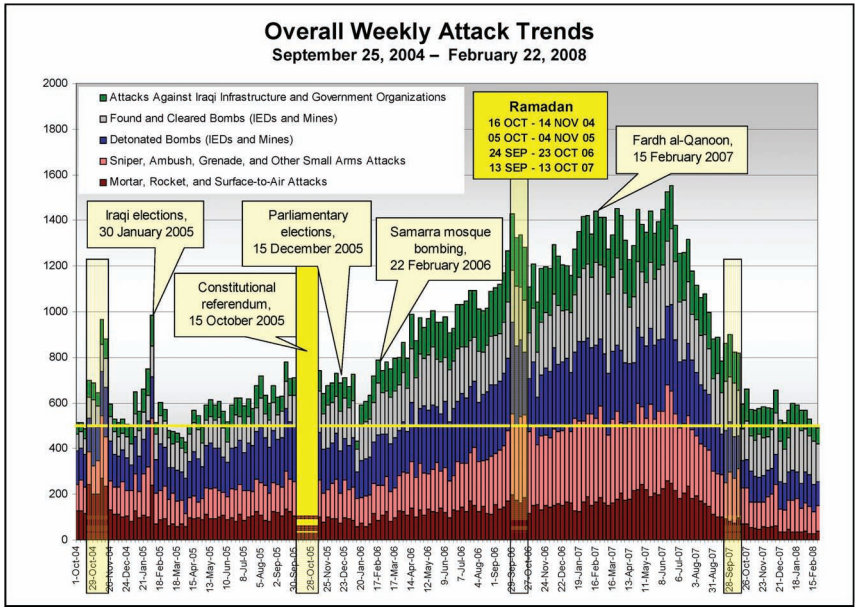
The *total* levels of violence declined significantly in early 2008 from their peak in the summer of 2007. Attacks against Iraqi infrastructure and government organizations also declined, as did detonated IEDs and mines, direct-fire attacks (snipers, ambushes, RPGs, and so on), and mortar and rocket attacks, as shown in Figure 6.2. This has resulted in fewer Iraqi civilian deaths and fewer U.S. and Iraqi military deaths.[6] In addition, the number of weapons caches found by coalition and Iraqi forces increased dramatically over this same period.

However, the DoD attributes this decline to the increased operational tempo made possible by the troop surge, the growth of the

[5] These are typically copper slugs shaped by the detonation of the bomb to a form best suited to penetrate armor. They are often positioned to strike through the windows of passing vehicles, where there is less armor protection.

[6] U.S. Department of Defense (2008).

Figure 6.2
Violence Indicators in Iraq



SOURCE: Multi-National Force–Iraq (MNF-I) SIGACTS [Significant Activities] III Database (coalition reports only) as of February 23, 2008.
NOTE: The figure shows executed attacks and potential (found and cleared) attacks.
RAND *MG788-6.2*

Sons of Iraq and other indigenous movements to counter Al Qaeda in Iraq, and increases in the numbers and capabilities of Iraqi forces.[7] The absolute decline does not appear to reflect improvements that are directly attributable to enhanced network-enabled operations. (On the other hand, improved networking may have helped U.S. forces keep pace with enemy adaptations. At the very least, better networking may have helped units receive and act on tips provided by Iraqi civilians.) The natural experiment comparing the relative performance of units sharing the same area of operations also proved inconclusive. Although we could discern some improvements in performance by the later units occupying a given area of operations, several independent variables

[7] U.S. Department of Defense (2008).

interfered with our ability to attribute the improved performance to the network. Key among these independent variables was the enemy's initiative; the enemy enjoyed enough freedom of action to decide when to intensify operations, shift activities to an adjacent region, or reduce his operational tempo.[8] These circumstances confounded our ability to correlate a shift in friendly versus enemy-initiated incidents with the coalition's network-enabled operations.

Comparison of unit performance among units serving concurrently provided an ironic twist. Among four BCT-sized units serving in AOs of roughly similar size in the general vicinity of Baghdad, we found that the least network-enabled (a light infantry formation) performed better than a cavalry formation employing a state-of-the-art network when compared on the basis of IEDs discovered versus those that detonate causing harm and also on the ratio of blue- versus red-initiated incidents. Of course, our sample is small and may not represent the general experience. More important, many variables are at work within and between these brigades, so the correlation between improved networking and unit performance on the specific metrics we chose is indeterminate.

NTC and JRTC Training Data

For years, RAND has been involved with the two premier Army training centers, collecting data on unit performance as brigades and battalions complete their rotations through the training centers as part of their periodic qualifications and predeployment certification processes. Therefore, we looked at data from recent NTC rotations (March 2005 through March 2006) to see if we could discern the effect of unit networking. Unfortunately, the data did not support the sort of natural experiment we had hoped they would. We could not find enough directly comparable data to allow us to examine whether networked units fared better in training than their less-networked counterparts. However, we were able to analyze the correlations between the use of

[8] See, for example, Cloud (2007) and Tyson (2007).

digital systems and some mission performance measures at the company and platoon levels. We give an overview of the results here; complete details on the data and our analysis, including important caveats, are in Appendix C.

At the company level, use of digital systems was weakly correlated with overall performance, as reported by observers/controllers, as well as with timely performance of mission-related actions, particularly in the performance of QRF missions. There was also a weak correlation between finding and dealing with IEDs and communicating with joint and coalition forces, but the latter analysis, although statistically significant, was based on substantially fewer cases than were the other results.

There were more data covering the platoon level, but they were more heterogeneous, since there are multiple platoon types with correspondingly different missions. Surprisingly, the use of digital systems at the platoon level was not correlated with overall mission accomplishment, except when platoons participated in QRF missions. Then, there were weak correlations with good internal communication, particularly in avoiding fratricide (and with communication with other friendly forces in accomplishing the latter).

Appendix C has more details about further analysis that could be performed, but taking into account different unit types would probably greatly reduce the precision of any analysis because of the limited amount of data available from just one year of rotations.

CHAPTER SEVEN

Military Utility of Network-Enabled Operations: Officer Impressions of Network Functionality

We expected that officers with operational experience in theaters such as Iraq or Afghanistan would have reasonably clear opinions about the networks that they used. These opinions could potentially provide "inside information" about how well the network performed in enabling Army operations. To capture these opinions, we administered two surveys. The first survey sought to capture officers' impressions of their command, sustainment, fire support, intelligence, and informal networks without inquiring about specific applications. The second survey, sampling a wider officer population pool, gathered opinions about the network in terms of exemplar applications in use. The second survey inquired about these systems in terms of how well they facilitated the cognitive and social domain functions.

This chapter summarizes how the respondents characterized network functionality in each survey.

Discussion of First Survey Results

The first survey sought impressions of command, sustainment, fire support, intelligence, and informal networks with regard to their reliability (how often they were up and functioning), connectivity (the network's ability to link units with their headquarters and those other units with which they had to plan and coordinate), content (accuracy and timeliness of information on the net and its relevance to user's tasks), and functionality (the ease with which individuals could receive, transmit, and manipulate information on the network). We sought a macro-level

impression of how well Army networks operated regardless of the programs of record and specific technologies involved. In this survey, officers were asked to rate network performance on a scale from 1 (excellent) to 5 (poor).[1]

The Survey Population

We sought officers who had operational experience and we sought candidates at different stages in their careers. Therefore, we decided to survey company-grade officers in the advanced courses at Fort Sill and Fort Benning; former company commanders and battalion-level staff officers in the Command and General Staff College at Fort Leavenworth; and former battalion commanders and senior staff officers at the Army War College. Table 7.1 summarizes the characteristics of our respondents and Figure 7.1 summarizes their regions of service.

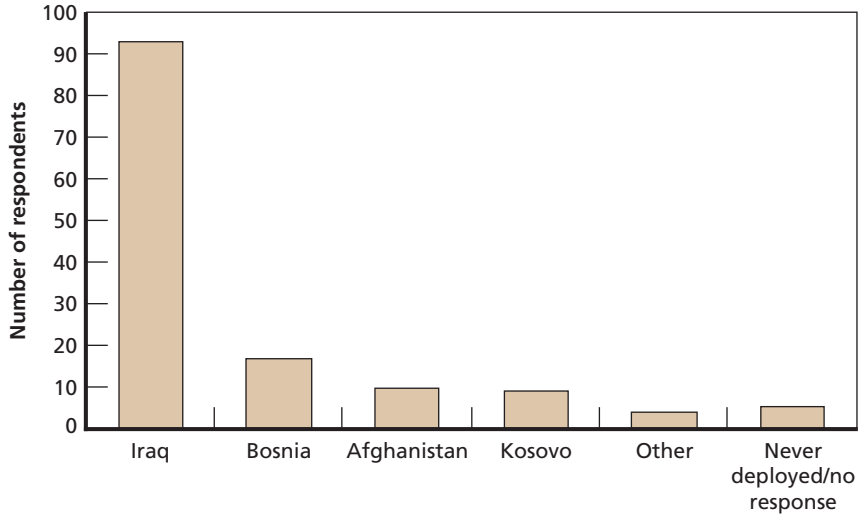
Table 7.1
Survey Respondent's Military Occupational Specialty

Rank	Infantry	Field Artillery	Other	Total
2LT	0	1	0	1
1LT	1	3	0	4
CPT	19	38	7	64
MAJ	6	7	20	33
LTC	0	5	3	8
COL	0	0	2	2
Total	26	54	32	112

NOTES: Fifty-seven percent of the respondents were captains and 29 percent were majors. Over 95 percent had served at least one tour overseas.

[1] The first survey instrument is available in Appendix A.

Figure 7.1
Distribution of Overseas Tours Among Respondents



RAND *MG788-7.1*

Assessments of Network Performance

Table 7.2 summarizes the overall evaluations of the networks with which the respondents worked. The scores suggest that experience with different networks differed somewhat in the field, which might

Table 7.2
Overall Network Evaluations

Network	Mean Rating	95 Percent Confidence Interval
Command	2.62	(2.48, 2.77)
Sustainment	3.03	(2.81, 3.25)
Fire support	2.68	(2.47, 2.90)
Intelligence	2.83	(2.57, 3.10)
Informal	2.51	(2.31, 2.71)

NOTE: 1 = excellent, 5 = poor.

reflect the nature of the theater of operations at the time the respondent served—was it an austere new theater, or an established one with mature, robust infrastructure to support an elaborate network?

Respondents generally reported better overall experiences with command and fire support networks and tended to be more critical of their sustainment networks. It is interesting to note that informal networks received the best overall ratings.

Most officers reported that they used informal networks because they were more reliable than the networks based on programs of record, they provided ease of connectivity, they offered functionality not available on the formal networks, and they made "doing my job" easier. The growth of informal networks and tools seems to have resulted from users' facility with technology, their familiarity with Web-based tools, and the their intuitive sense of where informal networks and tools could usefully supplement, complement, or supplant systems of record. Often, informal networks emerged when respondents imported commercial software to simplify command post tasks or to provide functionality that was absent from the systems of record.

Evaluation of Network Performance Metrics

The survey asked respondents to evaluate their various networks' reliability, connectivity, content, and functionality. Table 7.3 summarizes the ratings for each of these metrics.

The thought struck us that content and functionality might combine to represent sense-making—a critical activity of the cognitive and

Table 7.3
Summary of Average Network Performance, by Metric

Performance Metric	Mean Rating	95 Percent Confidence Interval
Reliability	2.27	(2.15, 2.39)
Connectivity	2.54	(2.34, 2.73)
Content	2.35	(2.22, 2.48)
Functionality	2.54	(2.41, 2.66)

NOTE: 1 = all of the time, 5 = none of the time.

social domains of the network that is central to this study. If content and functionality can combine to offer a proxy for sense-making or the network's ability to contribute to understanding, then the network's performance in this regard might be rated as mediocre.

Main Threads of Individual Officer Comments

As noted, most officers (77 of 112) volunteered additional impressions of network performance and value in the "comments" sections of the survey. These comments shared a few common themes. A consistent and important message was one of frustration. Although the message took slightly different forms (more senior officers tended to be more polite and conservative in their choice of adjectives), most comments expressed frustration at the limitations of the network. These included comments about unwieldy functionality that limited ease of use (28.6 percent), limited content relevant to their immediate tasks (5.4 percent), and too many screens to watch at once (2.7 percent). A companion desire was for simpler forms of communication over the net (17.9 percent), for example, simple voice radio and the ability to network instantly with key units (5.4 percent). Complaints about reliability emerged in 32.2 percent of written comments. Security concerns (too much security, 4.5 percent; too little, 2.7 percent) constituted the remainder of the written comments.

Overall Impressions of Network Performance

The officers surveyed rated their command networks as superior to the other programs-of-record networks: sustainment, fire support, and intelligence. Informal networks received the highest scores of all, however. More important, perhaps, there seemed to be a disparity between the way officers scored network performance in terms of reliability, connectivity, content, and functionality and the frustrations with network performance stated in their written comments. Performance scores according to the formal metrics were mediocre: 2.27, 2.54, 2.35, and 2.54, respectively. However, the preponderance of individual written comments seemed to judge network performance more harshly and tended to reflect an unsatisfied (although also unspoken) expectation about enhanced network performance.

Discussion of Second Survey Results

The second survey was designed to evaluate the physical, information, cognitive, and social domains of the network. The survey sought the opinions of officers who had recently deployed to Iraq or Afghanistan. Almost 7,000 officers in grades O-2 through O-6 in various combat and combat support branches were contacted by email and asked to complete the survey online.[2] Of those contacted, 1,613 (23 percent) responded to the survey; among these, 577 officers were disqualified because they had not deployed between 2000 and the time of the survey. The distribution of the eligible 1,036 (15 percent) officers by rank and branch are shown in Tables 7.4 and 7.5.

A majority of the eligible officers (85 percent) served in Iraq most recently (Table 7.6). Knowing the dates of overseas service for the officer respondents was important to ensure that the results indicated the networks deployed in Iraq and Afghanistan at the time of the study. We hoped to avoid biasing the response data with impressions drawn from earlier deployments where the networks might have been substantially more austere than those currently in place.

Table 7.4
Eligible Respondents, by Rank

Rank	No. of Officers	Percentage
O-2: 1LT	98	9
O-3: CPT	300	29
O-4: MAJ	252	24
O-5: LTC	240	23
O-6: COL	146	14
Total	1,036	100

NOTE: Percentages do not sum to 100 because of rounding.

[2] The second survey instrument is available in Appendix B. A complete description of our analysis of the second survey data is contained in Appendix C.

Table 7.5
Eligible Respondents, by Branch

Branch	No. of Officers	Percentage
Armor (AR)	164	16
Field Artillery (FA)	162	16
Infantry (INF)	147	14
Military Police (MP)	99	10
Ordnance (ORD)	127	12
Quartermaster (QM)	98	9
Signal (SIG)	154	15
Transportation (TRN)	85	8
Total	1,036	100

Table 7.6
Distribution of Officer Deployment to Iraq and Afghanistan

Deployed to	Time	No. of Officers
Iraq	Before November 2004	208
	After November 2004	668
Afghanistan	Before January 2006	64
	After January 2006	96
Total		1,036

We evaluated the state of each of the four domains on the basis of the officers' responses. Our analysis indicates that some attributes of the network are insufficient to deliver see first, understand first, act first, and finish decisively capabilities to these officers. The following sections discuss the most critical or deficient aspects of the network. Responses to all questions are presented in Appendix B.

First, it is important to place the responses into the proper context. All of the answer choices were on a scale from 1 (low) to 5 (high).[3] One may judge an average of 3 as a good rating because it is the median on a scale of 1 to 5. However, 3 indicates "half of the time" or "somewhat" (see Table 7.7). One has to ask, Does a network that delivers needed capabilities half of the time empower officers to see first, understand first, act first, and finish decisively? Imagine, for example, that the speed of the Internet slowed down our work half of the time or if our cell phones transmitted only most of the time, i.e., 75 percent of the time. We would find such service performance unacceptable and would change providers.

What Do the Survey Results Say About the Physical Domain?

The physical domain is composed of the physical theater of air, sea, and land where military operations take place. It also contains the physical infrastructure that moves information. The infrastructure constitutes

Table 7.7
Qualitative Descriptions of the Quantitative 1-to-5 Scale

Quantitative Scale	Qualitative Descriptions			
1	None of the time	None of the time	Not at all	Not at all important
2	Less than half of the time	Less than half of the time	A little bit	A little important
3	Half of the time	Half of the time	Somewhat	Somewhat important
4	More than half of the time	More than half of the time	Quite a bit	Very important
5	All of the time	All of the time	Extremely	Extremely important

[3] This scale operates in the reverse direction of the one used in the first survey.

the "highway" on which the information travels, that is, the Internet, the electromagnetic spectrum, and so forth. This highway is built on and connects various network devices, such as phones, computers, radios, fax machines, and other devices that transmit and receive information. The officers were asked questions regarding their experiences with the physical quality of networking and network devices. In particular, the questions pertained to such attributes as reach, network capacity, responsiveness, flexibility, security, availability, and capabilities. After examining the officers' responses, we evaluated the state of the physical domain and summarized our findings. Results of all questions can be found in Appendix B. The discussions following the domain summaries focus on the most critical or most deficient aspects of the domain.

Summary of the Physical Domain

- Communication to non-U.S. units is reliable only half of the time.
- Half of the time, the speed of the network slows down the officers' work.
- Half of the time, the network is not adaptable to changing operational needs.
- Half of the time, the limited number of radios, phones, and computers affect operations.
- Overall, O-6 and Signal experience better reach and network capabilities than O-3 and combat branches.

The Physical Domain Is Not Adequate to Deliver See First Capabilities to the Officers

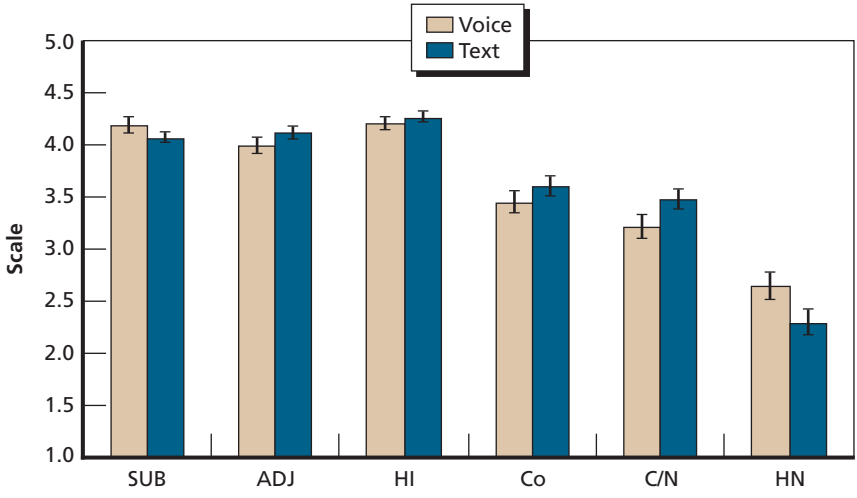
We found that although officers were able to reach other U.S. units (subordinate [SUB], adjacent [ADJ], and higher [HI]) by voice (phone, radio, voice over Internet protocol [VoIP], and so forth) and text (email, Internet Relay Chat [mIRChat], for example) "most of the time," they were able to reach coalition units (Co) and contractor/NGO (C/N)

groups only "half of the time," and host nation units (HN) even less than "half of the time" (Figure 7.2).

In addition to the low ratings, many respondents marked "N/A" for both voice and text communication with coalition, contractor/NGOs, and host nation forces (Figure 7.3). An N/A response may indicate that the officer did not have enough or any experience trying to reach these three non-U.S. military groups. This lack of experience may indicate barriers stemming from technical deficiencies or from habits of mind that are U.S. military-centric.

Although reliability of communication with contractors/NGOs and host nation units needs to improve greatly, analysis of officer responses shows that reliability has improved over time. The greatest improvement appears to have occurred between 2004 and 2005. Note that we did not have enough responses for host nation reach by text to perform a time analysis (Figure 7.4).

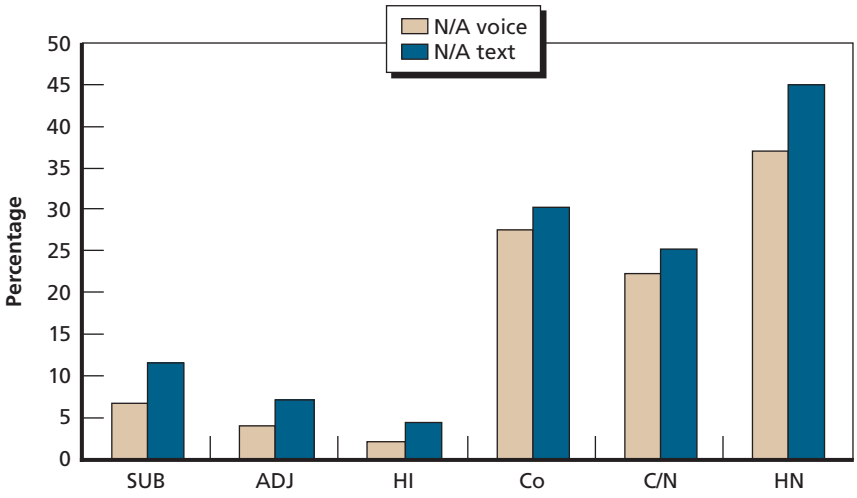
Figure 7.2
How Reliably Could You Reach Other Units Using Voice or Text?



NOTE: 1 = none of the time, 5 = all of the time.

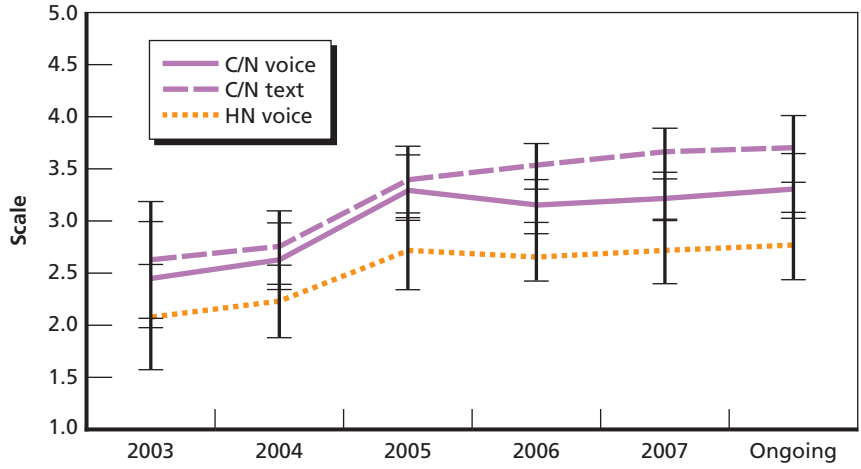
RAND *MG788-7.2*

Figure 7.3
Percentage of Respondents Who Marked N/A



RAND *MG788-7.3*

Figure 7.4
Reach Reliability with Contractors/NGOs and Host Nations Improved



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-7.4*

What Do the Survey Results Say About the Information Domain?

The information domain is where information is created, manipulated, and stored. There is a plethora of information in print, on the Internet, and in a variety of military databases, but more information does not equate to better information. A deluge of disorganized, unedited information can hide the "right" information and retard operational speed. The "right" information must be relevant to the task at hand, current enough to be useful, and derived from credible sources. These attributes are essential to compiling a complete set of information to aid sound decisionmaking.

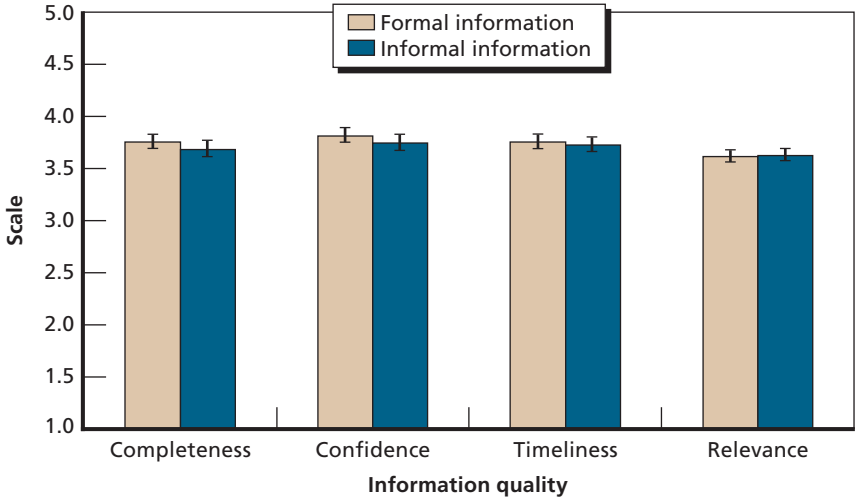
Soldiers in theater are obtaining and sharing information through informal sources, such as cell phones (voice, text, and data), mIRChat, Google Earth, and email. In light of the formidable challenges of irregular warfare, it is no surprise that soldiers are using these highly accessible informal media to obtain information that may partially lift the "fog of war" for them, rather than waiting for information to trickle down through formal channels. Hence, as the informal channels grow, it is important to compare the role they play relative to the formal channels. Understanding why soldiers turn to informal networks may help us understand the inadequacies of the formal networks (Figure 7.5).

Summary of the Information Domain

- The information domain is meeting the needs of the officers more than half of the time but still less than most of the time.
- Relevance of information needs the most improvement. There is no significant difference between the perceived quality of formal and informal information.[4]

[4] Formal information is defined as information obtained through formal systems. Formal systems are part of a program of record (for example, the Army Battle Command System [ABCS]) or are systems that may not have a program of record but were mandated to be used by higher commanders (for example, CPOF). Informal information is defined as information obtained from informal systems. Informal systems are ad hoc systems, generally advo-

Figure 7.5
Quality Comparisons of Formal and Informal Information



NOTE: 1 = none of the time, 5 = all of the time.
RAND *MG788-7.5*

- About half of the time, officers are finding in the informal network what cannot be found or is more difficult to find in the formal network.
- There is less digital divide than we thought. No significant differences across the ranks were found.

A little less than "most of the time," the information domain is meeting the needs of officers in the following ways: (1) They were able to obtain all the information they needed to accomplish their task, (2) they were confident in the accuracy of the information, and (3) the information was current enough to be useful. Furthermore, the survey group reported that most of the information they obtained was useful. These ratings indicate that the information domain is helping the officers accomplish their tasks.

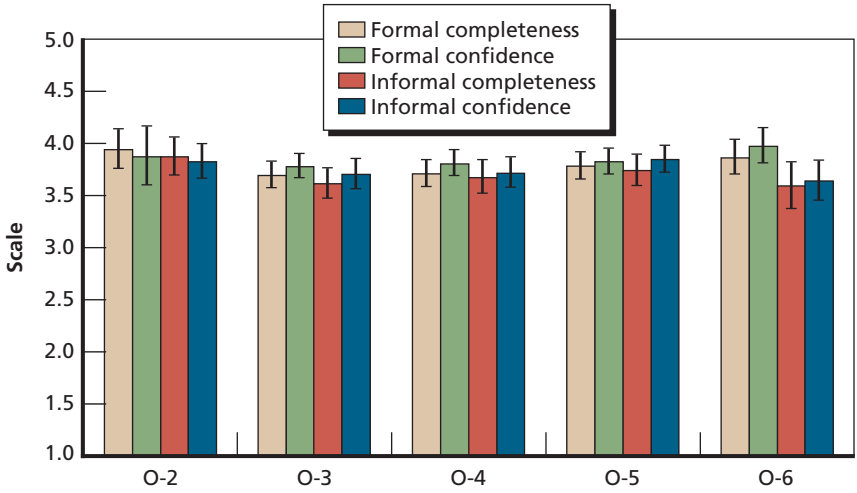
---

cated by the lower echelons and pushed to higher echelons (for example, mIRChat, Google Earth, and soldier blogs).

What is striking is that there is no significant difference between the quality of formal and informal information. Further comparisons between formal and informal information by rank show no significant perceived difference between the two types of information. The only exception is the confidence at the O-6 level in the accuracy of the information. Colonels expressed greater confidence in the accuracy of formal information than informal information. There was also no significant difference in the ratings of these information qualities across the ranks, indicating that there is less of an information or digital divide than one would have guessed between the lower and higher echelons (Figure 7.6).

About "half of the time," the officers used the informal network because it was easier to obtain information and to connect to than the formal network. More important, they indicated that they used it more than "half of the time" because it made their jobs easier. They also reported using the informal network because it offered functionalities

Figure 7.6
Completeness of and Confidence in Information, by Rank



NOTE: 1 = none of the time, 5 = all of the time.

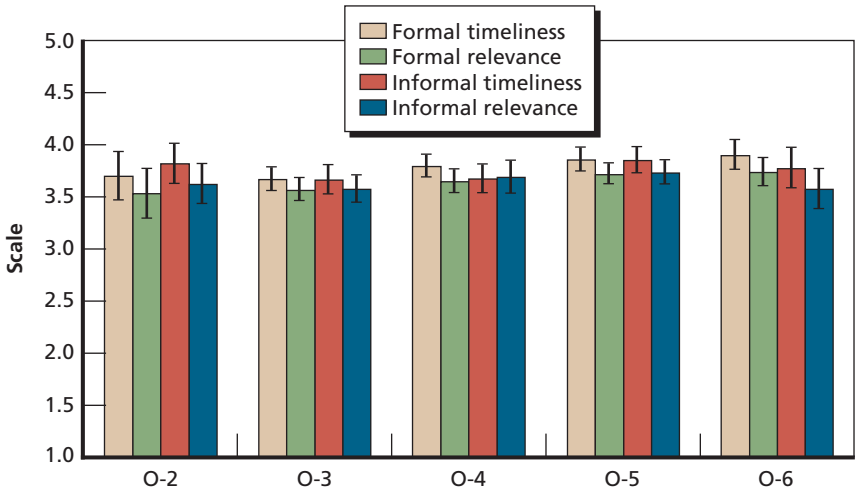
RAND *MG788-7.6*

not found in the formal network. The similarity between levels of use and reasons for use across the ranks is noteworthy (Figure 7.7).

Analysis by branch, on the other hand, revealed significant differences. Among the branches, Infantry found the informal network easier to use to a lesser degree than the other branches and therefore used the informal network least frequently (Figure 7.8). Perhaps it is for this reason that Infantry used the informal network least frequently among the branches. Interestingly enough, although Signal gave the highest ratings for informal information qualities, Quartermaster used the informal network significantly more frequently than Signal because of ease of connection and for greater functionality.

The digital divide between lower and higher echelons is not as wide as we initially thought. Regardless of their commanders' frequency of informal network use, lieutenants are using the informal network "half of the time." About "half of the time," officers found informal networks easier to use than formal networks, which is a significant contribution to their operational task.

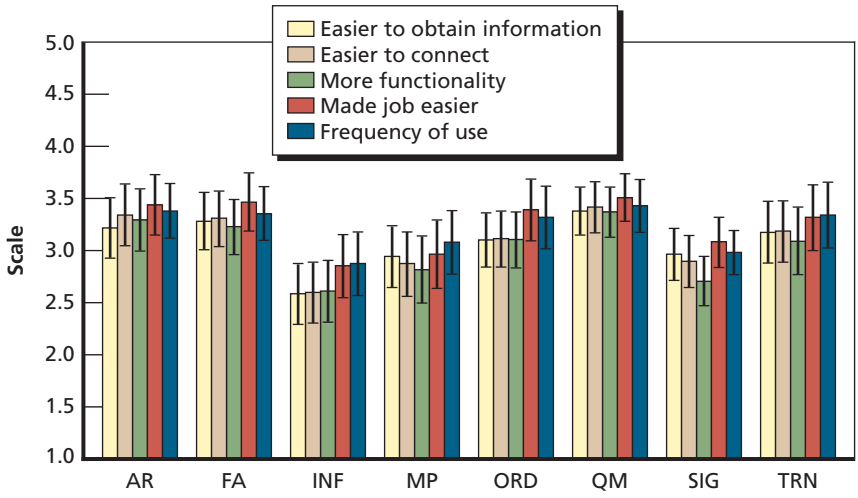
Figure 7.7
Timeliness and Relevance of Information, by Rank



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-7.7*

Figure 7.8
Reasons for Using Informal Network, by Branch



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-7.8*

What Do the Survey Results Say About the Cognitive Domain?

The cognitive domain is where sense-making—a process of awareness, understanding, and decisionmaking—occurs. The cognitive domain is a particularly challenging one to study and to measure because it occurs mostly within the mind of the soldier. Yet, the cognitive domain—in conjunction with the social domain—is where the network ultimately provides its value. Even if the physical and information domains were to be composed of the latest technology and the deepest database, they would be meaningless unless they enabled and empowered soldiers to observe, understand, decide, and act and thereby influence their environment in the fashion intended.

How quickly and how well an officer understands large amounts of information are influenced by the systems on which the information is presented. For this reason, we decided to ask questions regarding the cognitive domain for specific systems. A list of formal systems was pre-

sented and the officers were allowed to choose as many systems as they wanted to critique. The systems included the ABCS, other command and control systems, and some logistic systems. Although SIPRNet is not a system per se, it is a very popular information conduit and therefore was included on the list. The descriptions and functions for each system are found in Appendix B. The systems that received the highest number of responses were SIPRNet, FBCB2, and CPOF, in that order.

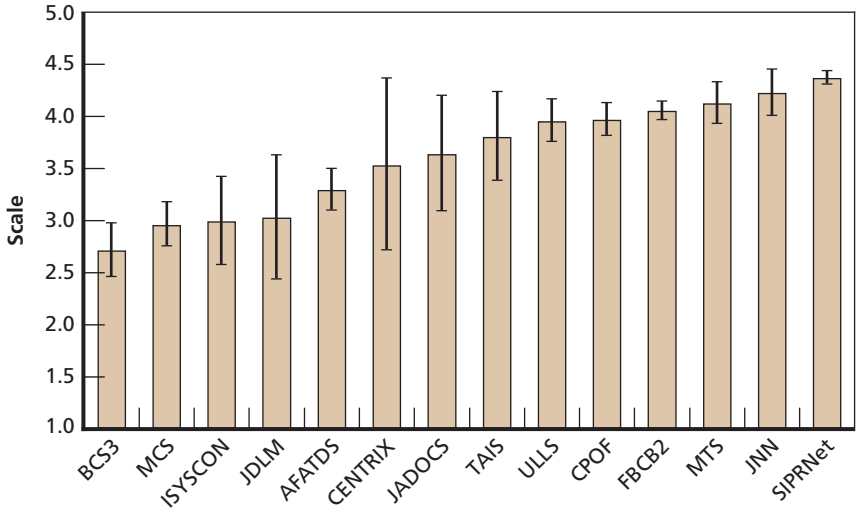
Summary of the Cognitive Domain

- Most of the time, officers were able to understand all of the formal and informal information needed to accomplish their tasks.
- Some systems improved the sense-making process "most of the time."
- The degree of improvement in sense-making depends on the specific systems and the quality of system.
- Formal systems need to be designed to deliver understand first, act first capabilities to the cognitive domain.

Across rank and across branch, the officers uniformly reported that they were able to understand all of the information needed to accomplish their tasks "most of the time." No significant difference between formal and informal information appeared in our analysis.

The survey results show that different formal systems have varying degrees of importance in the sense-making process. When asked how important the systems were to their situational understanding and to their decisionmaking processes, the officers' responses ranged from "a little important" to "very important." Some of the systems they rated less important were Battle Command Sustainment Support System (BCS3), Integrated System Control (ISYSCON), and Advanced Field Artillery Data System (AFATDS), programs of record of the ABCS family of systems. Some of the systems receiving higher ratings were not programs of record, such as CPOF; one—SIPRNet—is not a system per se but a Web medium. (Another, Joint Network Node [JNN], is a satellite conduit for information and other applications.) See Figure 7.9.

Figure 7.9
How Important Was the System to Your Situational Understanding?

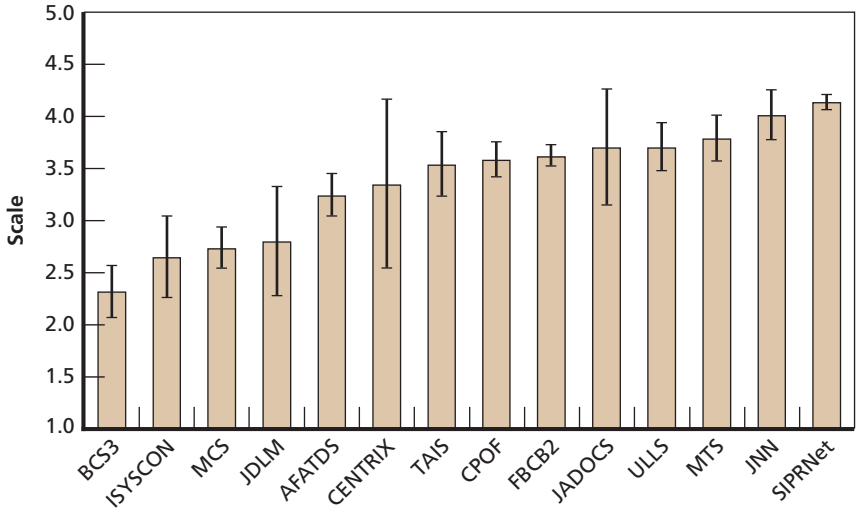


NOTE: 1 = not at all important, 5 = extremely important.
RAND *MG788-7.9*

The survey results suggest that formal systems can improve the sense-making process. In the cases of the three most reported systems (SIPRNet, FBCB2, and CPOF), the officers expressed that "most of the time," these systems helped them to understand the information faster, more fully, and more completely than would have been possible without the systems. Likewise, the systems raised their confidence "most of the time" that their situational understanding was correct. Given these results, it is no surprise that the officers regarded these three formal systems as "very important" (3.96–4.36) to their situational understanding. The mean ratings of these systems are presented in Figure 7.10. Among these three systems, SIPRNet received the highest ratings, and its ratings were significantly different from the ratings of FBCB2 and CPOF.

Our research shows that the quality and performance of the formal system affect officers' decisionmaking processes. How confident the officer is in his/her situational understanding is an important precursor to decisionmaking, which in turn is a prerequisite to acting

Figure 7.10
How Important Was the System to Your Decisionmaking Process?



NOTE: 1 = not at all important, 5 = extremely important.
RAND *MG788-7.10*

first. The speed of the decisionmaking process affects whether U.S forces initiate the engagement or react to an enemy initiative. Among SIPRNet, FBCB2, and CPOF, SIPRNet allowed officers to make decisions faster than they would have without the system and more frequently than with the other systems. Officers in combat units at the battalion and below level found SIPRNet helpful to a lesser degree than did officers in combat support units above battalion.[5] This may be because SIPRNet was not, at the time of this study, typically available at echelons below battalion. (We have subsequently learned that units at the company level have begun to receive SIPRNet access.)

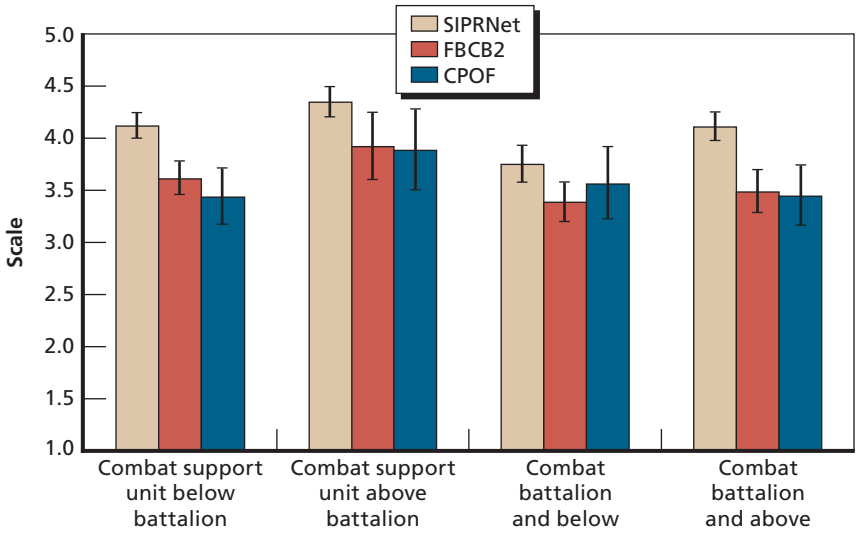
How confident the officer is in his/her decision may also influence how decisively the operation is executed. The officers reported that the

[5] Because we did not receive enough responses to analyze the data by rank and by branch, we aggregated the rank by battalion and below (LT, CPT, and MAJ) versus above battalion (LTC and COL) and branch by combat (INF, AR, and FA) versus combat support (MP, ORD, QM, SIG, and TRN), resulting in the four groupings.

three aforementioned systems were "very important" in raising their confidence in the correctness of their decision. The distinctions in level of importance among the three systems were not significant. The officers in different echelons and branches did not differ significantly in the level of importance they placed on the system's role in raising their confidence.

The officers rated all three systems as "very important" to their decisionmaking process (Figure 7.11). Among the three systems, SIPRNet was rated the highest. It may be that SIPRNet has the widest reach among these systems. It is also the most flexible and open-ended tool, providing access to dozens of databases scattered among units and headquarters in theater and hundreds of databases outside theater. SIPRNet also provides a way to access many informal tools developed by talented individuals throughout the military and intelligence communities to enhance their effectiveness.

Figure 7.11
How Often Did This System Help You Make Your Decision Faster Than You Would Have Without the System?



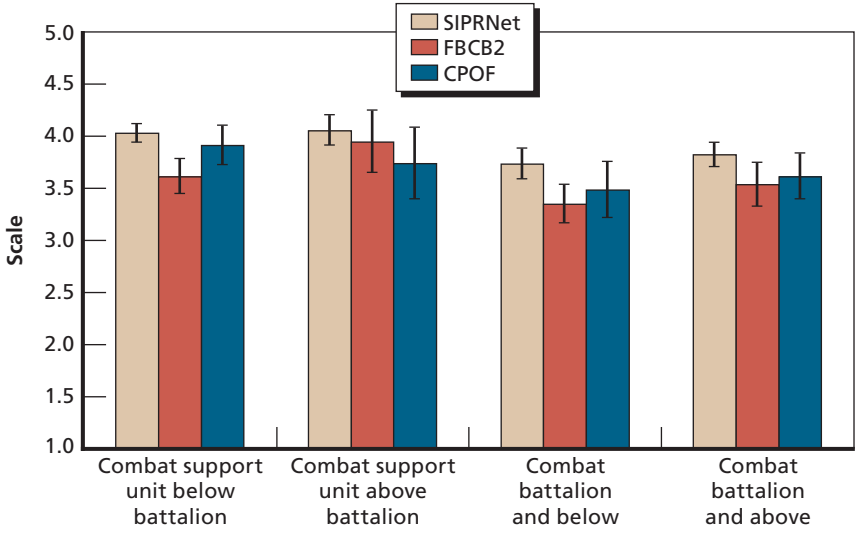
NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-7.11*

Officers in combat support echelons above battalion placed more importance on the systems than did combat battalion and below officers (Figure 7.12). It is also noteworthy that combat battalion and below is the group that FBCB2 was designed to serve, yet this group gave the lowest ratings to FBCB2 among the four groups. Our analysis indicates that the formal systems can enhance the performance of the cognitive domain, thereby helping officers to understand first. Although the cognitive domain resides in the minds of the officers, it can be matured by enhancing the performance of these formal systems. It may be more cost- and time-effective to design better formal systems in some cases than to improve the cognitive skills of officers and enlisted soldiers who are already heavily, if not over, tasked.

The survey results indicate weak to moderate correlations between the user-friendliness of the systems and how well the systems aided sense-making (Table 7.8; Figure 7.13).

Figure 7.12
How Important Was the System in Raising Your Confidence That Your Decision Was a Correct One?



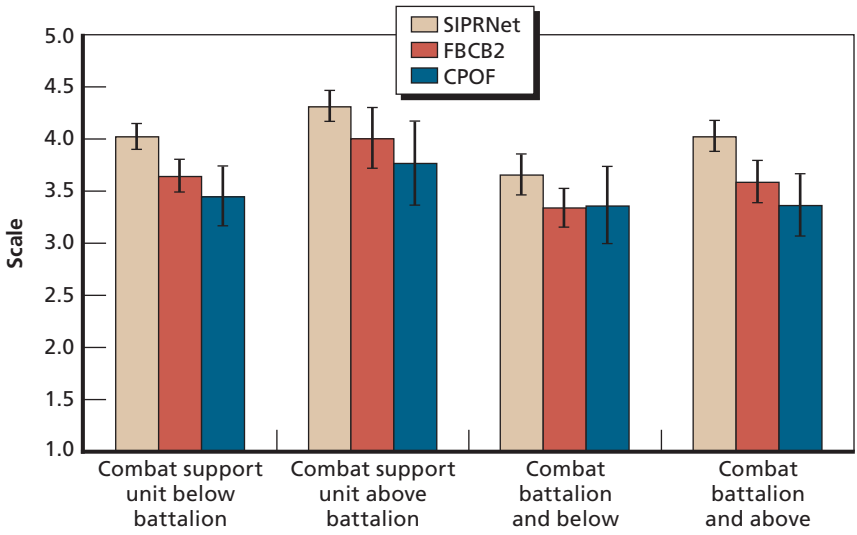
NOTE: 1 = not at all important, 5 = extremely important.

RAND *MG788-7.12*

Table 7.8
Correlations Between Cognitive Domain Attributes and System User-Friendliness

Cognitive Domain Attribute	SIPRNet	FBCB2	CPOF
Understand completely	0.45	0.48	0.62
Understand faster	0.45	0.44	0.62
Faster decisionmaking	0.43	0.41	0.6

Figure 7.13
How Important Was the System to Your Decisionmaking Process?

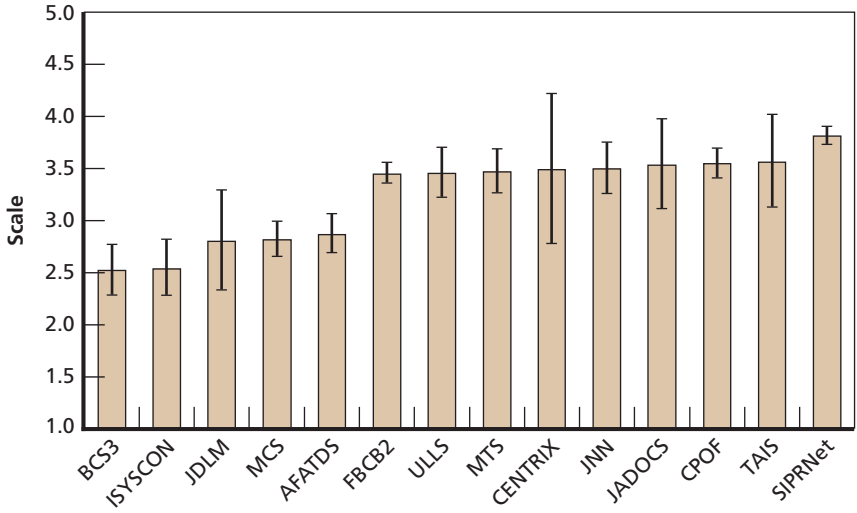


NOTE: 1 = not at all important, 5 = extremely important.

RAND *MG788-7.13*

Overall, the user-friendliness of the systems was not rated very highly (Figure 7.14).

Figure 7.14
To What Degree Was the System User-Friendly?



NOTE: 1 = not at all, 5 = extremely.
RAND *MG788-7.14*

What Do the Survey Results Say About the Social Domain?

Military operations are inherently social, drawing on formal relationships, habitual associations, and collective practices codified in field SOPs to forge unity of action through careful cooperation and communication. Therefore, it is important that individuals and units share information. In current theaters of operation, it is becoming more and more important for U.S. forces and non-U.S. forces to share information. U.S. forces are conducting SSTR operations in a foreign land of which they have limited cultural understanding. To succeed in these theaters, U.S. forces must rely on non-U.S. forces, such as the leaders of the local population or NGOs working closely with local populations, to see first and relay information to U.S. forces.

To achieve unity of effort, the distinct, individual understandings must merge into one shared understanding. This merging can be particularly challenging for geographically dispersed units. Formal systems may help achieve shared understanding by providing information and visual representations of the battlespace.

Summary of the Social Domain

- Officers are pushing information more frequently than they are receiving information from other units.
- Combat battalion and below personnel are pushing and receiving information about half of the time; for other groups, it is most of the time.
- There is no significant difference in frequency of formal versus informal information being exchanged.
- Formal systems facilitate information-sharing and establish shared situational understanding among U.S. forces more frequently than with coalition and host nation units.
- Overall, SIPRNet facilitates information-sharing and establishes shared situational understanding better than other formal systems.

The Social Domain Needs to Better Include Coalition and Host Nation Partners in the Information Exchange

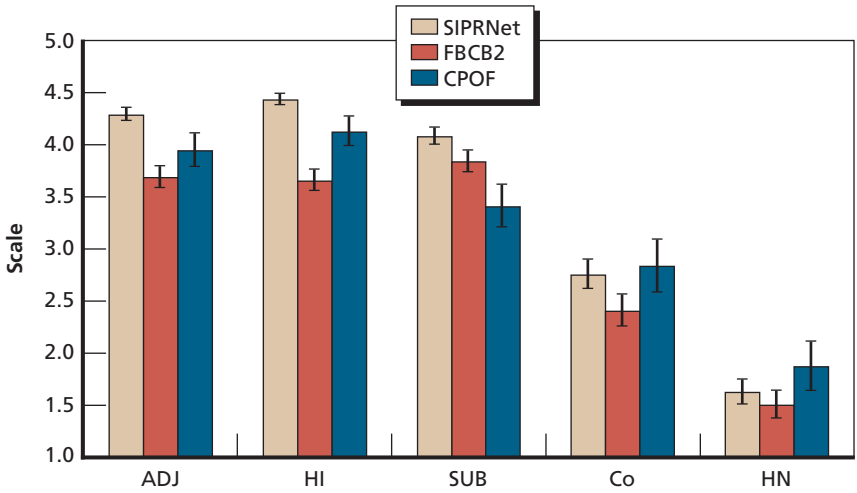
The survey results indicate that officers are pushing information a little less than "most of the time" and are receiving information from others a little more than "half of the time." It is unclear whether higher frequency of information-pushing would lead to greater mission effectiveness. The relatively moderate ratings may reflect officers selectively pushing high-quality information. Increasing the frequency of sharing marginal information may actually be counterproductive to the overall mission. Interestingly enough, officers are pushing and receiving formal and informal information at similar frequency. This behavior reflects the fact that the officers' opinions of the quality of formal and informal information are similar, as discussed in the information domain section of this chapter.

The frequency with which officers pushed or received information may be influenced by how easily they were able to share the information. Our results show that formal systems facilitate the sharing of information to different degrees. Moreover, using the same formal systems, officers are able to share information with different units at varying ease (Figure 7.15). SIPRNet facilitated sharing with U.S. forces better than FBCB2 and CPOF. However, CPOF facilitated sharing with coalition and host nation units to a similar degree as SIPRNet. In order of decreasing ease of sharing, SIPRNet, FBCB2, and CPOF facilitated sharing with other units in the following order:

SIPRNet: higher > adjacent > subordinate > coalition > host nation
FBCB2: subordinate > adjacent and higher > coalition > host nation
CPOF: adjacent and higher > subordinate > coalition > host nation.

The systems also varied in how well they established shared situational understanding with different units. SIPRNet was better than

Figure 7.15
How Reliably Did the System Facilitate Sharing of Information with Other Units?



NOTE: 1 = not at all, 5 = extremely.

RAND *MG788-7.15*

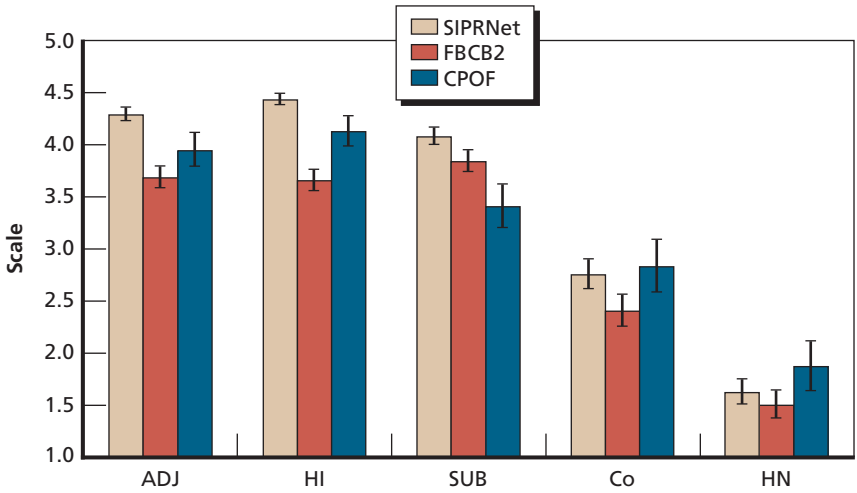
the other systems at establishing shared situational understanding with U.S. forces, but all three systems performed poorly in establishing shared situational understanding with coalition and host nation units.

The survey results reflect the challenges involved in sharing information and arriving at a common situational understanding with non-U.S. partners (Figure 7.16). Issues of security, interoperability, and availability of formal systems hinder achievement of a level of interaction on a par with that among U.S. forces. Informal networks and informal systems may be one temporary solution to bridging the gap. Further research and development are needed to explore how informal networks and informal systems can bring the non-U.S. units into the circle without jeopardizing mission security.

Summary of the Survey Results

Our survey of Army officers returned from operational deployments suggests that they are marginally satisfied with network performance,

Figure 7.16
How Often Did This System Establish Shared Understanding?



NOTE: 1 = not at all, 5 = extremely.

RAND *MG788-7.16*

although many acknowledge some performance limitations and expressed interest in additional functionality.

The survey revealed that the speed of the network and limited supply of network devices affected operations half of the time. The officers also reported that the network was not adaptable to changing operation needs half of the time. Among various units, communication with contractor/NGOs, coalition, and host nation units provided contact "half of the time" or "less than half of the time."

The quality of the information needs improvement. The officers report that the information quality is meeting their needs more than "half of the time" but less than "most of the time." The officers regarded informal information to be just as good as formal information. Informal information and informal networks play important roles in the operations.

The formal systems differ greatly in how quickly and how well they help officers gain situational understanding. Formal systems also differ in how well they facilitate sharing of information and establishing shared situational understanding between units. Not surprisingly, SIPRNet, FBCB2, and CPOF were among the systems that garnered the greatest number of responses as well as the highest ratings in performance.

We also gained some insights into several more specific questions of interest to our study, which are discussed below.

Does Better-Quality Networking Lead to Improved Information-Sharing?

The ability to reliably reach other units is an indication of good-quality networking. How often officers are pushing information and receiving information are measures of information-sharing. When these two sets of results were tested, we found no correlation between them. At least judging by our survey results, reliable reach does not necessarily lead to more sharing of information. However, we did find a strong correlation between how often officers share information and how often they receive information. This correlation suggests that one act encourages the other. Hence, efforts to improve information-sharing may not have

to be two separate lines of effort because it appears that sharing is an act that encourages imitation.

Does More Information-Sharing Lead to Improved Information Quality?

We measured information quality based on completeness of information, timeliness of information, and confidence in the accuracy of the information. Our tests indicated only weak positive correlations between how often officers pushed or received information and their responses to the quality of information questions. This was true for both formal and informal information. However, we did find a slightly stronger correlation for informal information (0.52–0.58) than for formal information (0.3–0.49). We also found strong correlations among the completeness, timeliness, and confidence in the accuracy of informal information (0.75–0.84).

Does More Information-Sharing Lead to Improved Individual Understanding?

For formal information, there is a weak positive correlation (0.53–0.66) between the quality of information (completeness, timeliness, and confidence) and how often the officers were able to understand all of the information they needed to accomplish their tasks. However, a strong positive correlation (0.73–0.79) was evident between the quality of informal information and individual understanding.

We also found weak positive correlations between SIPRNet's ability to facilitate information exchange with adjacent, higher, and subordinate units and how often SIPRNet helped officers to understand information faster and more completely (0.52–0.58). Weak positive correlation was found also for FBCB2 (0.48–0.64) and CPOF (0.41–0.68).

Does More Information-Sharing Lead to Improved Shared Understanding?

We also tested whether a connection existed between SIPRNet's ability to facilitate sharing of information and its ability to establish shared understanding. We found a weak positive correlation between

information-sharing with adjacent units and establishing shared understanding with adjacent units (0.62). The same was true for higher units (0.62). Strong positive correlations were found for subordinate, coalition, and host nation units (0.78, 0.84, and 0.87, respectively). Similar trends were found for FBCB2 and CPOF.

Does Improved Individual Understanding Lead to Improved Decisionmaking?

Our analyses indicate a strong positive correlation between individual understanding and improved decisionmaking. SIPRNet's ability to help an officer understand information faster and more completely correlated strongly to its ability to help officers make decisions faster and feel more confident about their decisions (0.69–0.75).

Strong positive correlations are present between FBCB2's ability to help officers understand faster and more completely and to help them make decisions faster (0.73 and 0.7). There was a moderate positive correlation to raising their decision confidence (0.67 and 0.64). Similar correlation trends were found for CPOF.

Does Improved Shared Understanding Lead to Improved Decisionmaking?

In the case of SIPRNet, a strong positive correlation exists in how often shared situational understanding is established in the unit, how often the officers made decisions faster, and how often they were confident in their decision (0.72 and 0.69). Shared situational understanding with other U.S. units was weakly and positively correlated with faster decisionmaking and confidence in decisions (0.55–0.66). Similar correlation trends were observed for FBCB2 and CPOF.

CHAPTER EIGHT

Options to Enhance Network Performance

This chapter examines options for enhancing network performance to better prosecute MCOs, SSTR operations, and irregular warfare operations. We begin with some observations of the network's strengths and weaknesses from the analyses discussed in the previous chapters. We then describe where the greatest opportunities may exist for the network to enhance operations—in enabling peer units to self-synchronize and headquarters to conduct electronic warfare. We then describe a notional example of how the cases described in Chapter Five might have turned out for the better had these capabilities been available to the units involved. We conclude this chapter with some implications of our analyses for potential changes to Army network DOTMLPF.

Observations from Case Studies, Data Mining, and Surveys

If we overlay what we learned from the data-mining on the responses from the officer surveys and case studies described above, a number of observations about network performance emerge. In short, the network is clearly better at some tasks than at others.

The Network's Strong Suit

The network performs well in its role producing blue situational awareness (Where are my buddies?). Situational awareness is good for most combat units in Iraq, and new concepts, such as "electronic over-

watch" (described below), could improve situational awareness and turn ambushes into opportunities to destroy the enemy. Generally speaking, it appears that when U.S. units enjoy the initiative, the network functions well to orchestrate their activities.

Said somewhat differently, the network does reasonably well at generating unity of action among units in conditions under which those units have the initiative. The connectivity provided by the network usually allows units, typically at the battalion and brigade levels, to coordinate and synchronize their efforts, and the network appears to have the potential to extend these benefits downward to lower echelons of command. The network supports information-sharing and, perhaps most important, adapting operations when the original plans must be replaced quickly with a more suitable approach. Under such circumstances, the network appears very useful in developing and disseminating alternative plans to subordinate units.

Where the Network Proves Less Capable

When the enemy enjoys the initiative, network benefits to U.S. and coalition forces appear more modest. In particular, the network has proven less useful in detecting and identifying insurgent forces before they strike. As the case studies suggest, there is much room for improvement in this regard—improvements that could result from adapting current TTPs and unit practices. The network has not demonstrated much additional utility for determining insurgent capabilities and intent and thereby supporting the interdiction and destruction of irregular enemy forces.

The stability and security operations (sometimes called phase four) environment seems particularly difficult for the network. The network contribution to identifying and locating the enemy and helping U.S. forces make sense of their operating environment seems uneven—helpful in specific operational concepts (for example, TF ODIN) or in particularly well-equipped units (Special Forces or Stryker) but less helpful for protecting convoys and combat outposts. The network does not prove as useful as it might in helping U.S. forces deny the initiative to the enemy.

Network Performance "Bottlenecks"

The physical and information domains are relatively well developed in Iraq and Afghanistan today. In some of the earlier cases, units lacked adequate communication networks for voice and data—particularly over long distances while on the move. Over time, though, they have positioned themselves in fixed locations with better access to landline, satellite, and other wireless communication, and the Army has pushed powerful network systems to lower echelons. These include the DCGS-A down to brigade level, SIPRNet to the company level, and BFT to the squad level. Note, though, that communication gaps still crop up from time to time, particularly for small units on the move away from their bases. These issues may become crucial in future conflicts if most units are on the move, widely dispersed, and far from fixed bases.

With access to communication comes access to information. Blue Force Tracker provides a real-time situational awareness of blue forces. Command Post of the Future provides a command network with superior, subordinate, and peer units. SIPRNet opens up hundreds of databases in theater and around the world. New sensors—such as the UAS—will add much more data to these databases, and the DCGS-A will open more of these databases to the vast collection capabilities of national and theater systems.

The challenge now is in using these networks and databases to enable better maneuver, fires, and other operations. Soldiers and commanders need better tools and skills to extract a few kernels of information from terabytes of data that may exist in each database. Fortunately, several emerging capabilities are beginning to provide help: new Army and DoD initiatives, informal systems and networks, self-synchronization, and electronic overwatch.

New Army and DoD Initiatives

The first of these emerging capabilities is made up of a mix of diverse initiatives begun by the Army, the other services, and other offices within

the DoD. Over the past few years, the Army has begun to deploy small teams that bring specialized capabilities down to the brigade level. Once at the brigade level, these teams are deployed with other tactical forces to support COIN operations. The first of these are the Human Terrain Teams. These teams consist of military officers and social scientists with the mission of "diagramming the cultural landscape."[1] Working directly for the brigade commanders, these teams help soldiers understand the nuances of local culture. USCENTCOM has validated a joint urgent operational needs statement for Human Terrain Teams to support each brigade. A second example is Cryptologic Support Teams, organized from the Army's military intelligence brigades.[2] These teams deploy in support of brigade commanders and have been credited with providing capabilities that are key to countering insurgent activities.[3] As a final example, the Army has stood up a Biometrics Task Force with the mission of acting as the DoD proponent for biometrics, leading the development and implementation of technologies, delivering capabilities, and improving operational effectiveness on the battlefield. Among other things, the Biometrics Task Force is developing and administering an electronic database to support the storage, retrieval, and searching of fingerprint, face image, iris image, and voice print samples.

Informal Networks

Another of these emerging capabilities is the result of officers and enlisted personnel at every echelon developing new tools and techniques to mine databases for information that can help commanders. An excellent example of an informal application is the Artillery Portal—designed by a brigade staff officer to display past enemy rocket and mortar attacks and project locations from which future attacks

[1] Pryor (2007).

[2] Sweet (2007).

[3] Odierno, Brooks, and Mastraccio (2008, p. 52); Asymmetric Warfare Group (2006); Tait (2007).

might be launched. Later, it was modified to include enemy direct-fire and IED attacks. This application, with links to unit-unique databases that feed it, was then shared over SIPRNet with other officers in the parent division (Multi-National Division–North, commanded by the 1st Infantry Division at that time). This tool provided valuable information to the brigade commanders, saved soldier time in building daily battle update briefings, and helped soldiers avoid dangerous routes and areas.

Self-Synchronization

Ideally, the Army network would enable commanders to synchronize units vertically across echelons, horizontally across Army and joint units, and outwardly with allies, coalition partners, and host nation authorities and citizens. Ideally, once connected, a networked force can synchronize the operations of these dispersed elements to see, understand, act on, and finish actions and tasks as a coherent force.

This is standard operating procedure during major combat operations, where unit commanders maintain tight situational awareness of units to their right and left flanks. However, tight and continuous awareness may be more challenging in distributed operations in which a given unit has been operating far from other friendly units most of the time. Often, during irregular warfare and COIN operations, blue units just happen to meet—for example, combat forces are patrolling, moving, or fighting adjacent to each other; convoys are moving through a battalion's zone; or UAVs and other aircraft are patrolling in the vicinity of friendly forces. The network today can enable these units to synchronize activities using such network tools as SIPRNet or such battle command tools as FBCB2 or CPOF, and Blue Force Tracker.

For example, a commander planning a convoy movement might query the CIDNE database to see where enemy activity has been high recently. He might then choose routes to avoid contact with an enemy given the latest information regarding recent enemy attacks. The convoy commander is normally expected to file a movement order, or "trip ticket," detailing the mission and destination, the composition of

the convoy, the call sign and command frequencies, and the intended route. The commander can then publish this ticket on SIPRNet and even push the information (for example, by SIPRNet email) to the battalions whose area of operations will be entered.

If BFT is on at least one (or better yet several) of the escort vehicles, the convoy commander can use it to monitor the locations of other U.S. units and to broadcast the convoy's own position as it moves. A key feature of BFT is a display showing a near-real-time picture of blue units' disposition using icons and unit labels.[4] At a minimum, this ability decreases the risk of fratricide. But BFT can also provide a free-text message that can provide substantially more information. For instance, a SLANT-type message can be broadcast by a U.S. unit, conveying[5]

- date time group
- unit identification, including the commander's call sign and command radio frequencies
- unit mission (for example, convoy on main supply route Tampa moving toward X)
- unit status (for example, troops in contact, or Mayday).

These same orders could then be automatically accessed by AO owners (using a "subscribe" procedure) to let them know which units will be moving through their area or operating in an adjacent area (for example, Company C, 2nd Battalion will move adjacent to the battalion zone, or a logistics convoy will move through the zone at 1900

[4] BFT has been criticized for having a long latency. It reportedly took up to 15 minutes during MCOs for icons to refresh on the BFT display—too long to reflect actual friendly positions in fast-paced maneuver warfare. Subsequent efforts have greatly reduced this latency. FBCB2-EPLRS (Enhanced Position Location Reporting System) provides this capability with less latency when subordinate units are within single- or multiple-hop EPLRS radio range. However, FBCB2 is available to a small percentage of U.S. units and not typically deployed with the Marines or allies.

[5] SLANT messages are used to give the commander accurate and routine information regarding the status of critical personnel and equipment necessary for the unit's operation to succeed. It can be submitted when necessary or as directed. The commander designates the information to report during planning or in accordance with unit SOPs (see HQDA, 1988, 1996a).

hours). At the beginning of every day, the battalion headquarters staff can download the trip tickets for convoys or other units due to move through their AO over the next 24 hour period.[6] As the convoy enters the battalion's zone, the battalion might integrate the convoy BFT transmissions with its own COP. In effect, the convoy commander might "check in" with the HQ staff as the convoy enters the AO.

Together, these pieces of information can provide a powerful tool for a battalion commander in charge of securing an AO. Convoy commanders might change their routes dynamically if enemy forces were suddenly spotted on the road ahead. On the other hand, combat and security forces may choose routes to block enemy forces or to seek contact on terms advantageous to U.S. or coalition forces. In some situations, the AO battalion might also choose to perform route reconnaissance or assign extra combat forces to augment convoy escorts.

The same pieces of information might help commanders synchronize the operations of maneuver units brought together by chance. Tactical units regularly file movement, maneuver, and fires plans that they send to their higher headquarters. Once these plans have been put on SIPRNet, they are, in principle, available to other units that are adjacent or may move into proximity. Battle command and situational awareness tools (for example, FBCB2, CPOF, and AFATDS) could be helpful in displaying the planned movements of adjacent units and in reminding warfighters where to look for friendly forces. For example, a battalion headquarters might plan to receive BFT transmissions from units operating in an adjacent AO for the next 24 hours. ("We will support them if they are heavily engaged and will request their support if one of our adjacent units is engaged.")

In a similar fashion, aircraft operations (Army, joint, or combined) should be knowable over a given zone (for example, a U.S. Air Force [USAF] UAV has flown over the battalion zone), by accessing the air tasking order (ATO) by way of the Theater Battle Manage-

[6] This information-sharing could be automated—for example, planned movements could generate automatic alerts much like the calendar reminders in many email programs.

ment Core System.[7] The zone owners could use both types of information to shape their own fire, maneuver, surveillance, or other plans; for example, receive a direct downlink from a USAF UAV tasked on ATO to be overhead from 0100 to 1200; the battalion will use any chance detections to observe or target and attack enemy forces, as best suits the commander's intent.

Electronic Overwatch

As we have seen in some of the cases discussed in Chapter Five, U.S. forces are surprised from time to time by the presence or actions of enemy forces. In some of these cases, the enemy presence might have been known or knowable by the command post or headquarters, but that awareness was not passed to the U.S. forces that came into contact. The idea is that one of these headquarters or command posts might be assigned the task of monitoring information relevant to units operating in a given area. The "overwatch" headquarters would be responsible for pushing vital information to the units in question; for example, putting red force information on the common operational picture. For these approaches, the overwatch headquarters will need to ensure that one of its elements has been tasked to monitor the surveillance assets employed and alert the assigned ground forces. Such an alert might be transmitted by voice, or it could be provided by way of a red force entry onto the battalion COP.[8]

Brigade and battalion HQ might provide electronic overwatch by passing red force location and information to subordinate commanders via FBCB2-BFT or by providing general information over voice radio. They should also be prepared to provide alerts to units moving into or

---

[7] New systems, such as the Heterogeneous Urban RSTA Team—under development by the Defense Advanced Projects Agency and the Army—might be useful for this purpose. See Pagels (2008).

[8] The Marines developed a concept similar to this with the Tactical Fusion Center, in which a given intelligence officer was assigned responsibility for a rifle regiment. In the Army, the 101st Airborne (Air Assault) Division reported to us that they provided overwatch of convoys and other 101st unit movements within their AO.

through their area of operations. Company and platoon commanders should be able to notify adjacent ground units and their higher-echelon commanders regarding contacts with enemy forces and intelligence, surveillance, and reconnaissance information gathered in the course of their operations.

Echelons above brigade (that is, division, corps, or Army HQ) have typically been assigned to monitor non-Army surveillance and reconnaissance assets, such as satellites and JSTARS, U-2s, Global Hawk, and other theaterwide aircraft. These higher headquarters must seek and push relevant information down to the brigade and battalion levels.

The brigade headquarters might be another place to monitor national and theaterwide ISR systems. To do so, the brigade will need the right direct downlink systems (for example, DCGS-A) and an intelligence section that can identify the portions of collected data pertinent to the brigade.

The brigade and battalion levels should also have the ability to anticipate and monitor UAVs and other ISR and combat aircraft controlled by other units or components (for example, the Combined Force Air Component Command) but flying over their AOs. In this way, headquarters and intelligence troops could exploit any intelligence, surveillance, and reconnaissance information generated in their assigned areas. Brigade and battalion headquarters also need the ability to operate and task their own UAVs, helicopters, and RSTA teams to conduct reconnaissance and surveillance. Information on enemy position, strength, and activities gathered from all of these sources should be passed to all subordinate units down to the platoon level. Company and platoon commanders should be able to downlink data directly from tactical UAVs that are flying overhead. They should also be able to access information from ground sensors, RSTA teams, and friendly units nearby.

Finally, commanders at every echelon need to be open to receiving actionable intelligence from host nation citizens. This might include anonymous tips given over a hotline to battalion, company, or platoon command posts; a direct statement by a willing informant; indications from observations of civilian traffic patterns or other behavior; or bio-

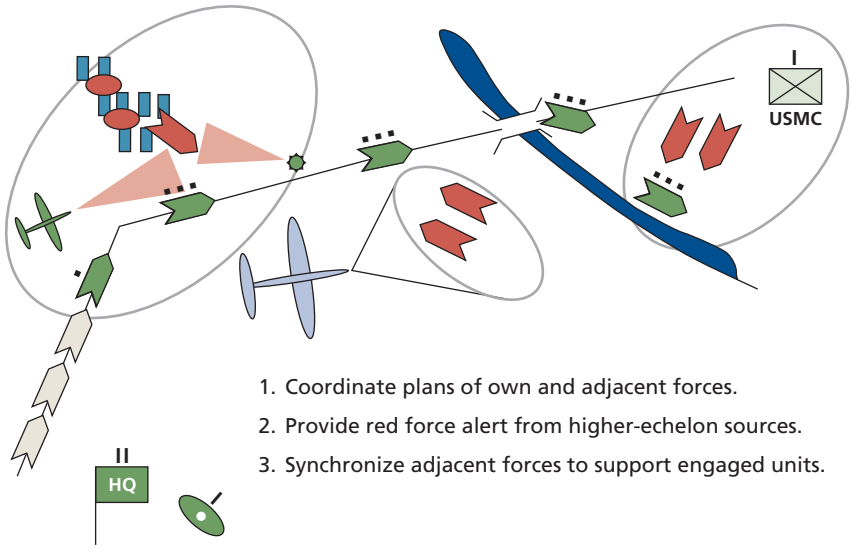
metric data from suspected insurgents that can be exploited to establish the identities of local "persons of interest." Some information from these sources can be used immediately; other information will need to be managed in a database able to handle a large amount of contextual information that will support sense-making as operations proceed. The goal is a real-time, complete display of information to ensure a common picture for all blue forces.

Applying Self-Synchronization and Electronic Overwatch

Synchronizing the operations of Army and joint forces to see first, understand first, act first, and finish decisively might include some of the elements described in Figure 8.1. This notional example might take place as a small part of a major combat operation, or it might reflect the daily operations of a battalion and its subordinate and adjacent units fighting irregular forces or conducting SSTR operations. Figure 8.1 depicts several activities taking place simultaneously.

At the left of the figure is a convoy moving through a zone under the control of an Army battalion. In anticipation of possible enemy action, the convoy parent unit has forwarded a trip ticket via SIPRNet to the headquarters of the battalions whose areas it will be moving through. In this case, the battalion AO headquarters has anticipated a potential enemy threat in a town close to the convoy's planned route. The battalion decides to conduct an electronic overwatch of the convoy, to be ready to provide it with support if it comes under attack within the battalion's area. In addition, the battalion commander believes that such an attack represents an opportunity to engage and destroy enemy irregular forces. Therefore, the battalion has placed unattended ground sensors with video cameras to watch the town. In addition, the battalion has ordered one of its maneuver platoons to patrol in the vicinity of the town and has directed one of its organic UASs to reconnoiter the area with a downlink to the platoon and battalion headquarters. The HQ will pass any alerts or other urgent information to the convoy via voice over the preestablished command frequencies.

Figure 8.1
Synchronizing the Operations of Subordinate, Adjacent, and Joint Forces



RAND *MG788-8.1*

The platoon commander receives the convoy SLANT report on his FBCB2 by way of Blue Force Tracker and knows when the convoy should enter the battalion zone. When the convoy enters the battalion's AO, it "checks in" with the battalion AO headquarters. The maneuver platoon receives this electronic check-in, and notes the entry of the convoy on its BFT. The platoon commander receives a direct downlink from the UAS and can see in real time what the UAS sees and receive a voice alert from the battalion overwatch element. The platoon commander also has the radio frequencies and call signs that the convoy commander escort vehicles are using, in case it becomes necessary to make direct voice contact.

At the same moment, a USAF UAS operates over the battalion. The battalion HQ knew when to expect the UAS because the Combined Air Operations Center sent out a flight plan to the headquarters units of the AOs that it would overfly. The battalion HQ began monitoring the raw feed from the UAS when it arrived overhead. (In cases

in which the battalion headquarters is fixed or has stopped moving, it may also be connected by SIPRNet to the UAS controllers.) The battalion HQ is also receiving alerts from an overwatch element at brigade headquarters regarding enemy forces found by this and other aircraft operating within the brigade sector. On this particular day, the battalion HQ sees enemy forces preparing an attack against one of its other maneuver platoons advancing along a major roadway. The battalion overwatch element alerts the platoon by voice (and also puts red icons on the battalion COP, which all platoons will see on their BFT), warns adjacent maneuver units to prepare to maneuver in support of an engaged unit, and orders an attached artillery battery to prepare to provide fire support.

Elsewhere in the battalion sector, a maneuver platoon is engaged by a numerically superior enemy force. The battalion overwatch element has received a troops-in-contact alert from the platoon. The battalion commander then orders additional forces to maneuver in support of the troops in contact, but it will be some time before they can reinforce. Fortunately, the battalion had previously synchronized its fire and maneuver plans with an adjacent Marine Corps infantry battalion. A Marine company in proximity has seen the troops-in-contact message from the engaged platoon and has received permission from its parent unit to maneuver and fire in support.

Counterfactual: Application of Self-Synchronization and Electronic Overwatch to Historical Cases

In this section, we describe ways in which the network concepts described in the preceding section might have been used to improve the capabilities of the units in each of our cases.

The 3-69th Armor

To begin, the 3-69th might have been helped by having better network access to the warning of enemy ground forces in the vicinity of the bridge. Warning might have been possible through various means, including direct downlink from JSTARS; voice warning from corps,

division, or brigade HQs; or red force posture indication on situational awareness tools, such as BFT. (The DCGS-A, when fully deployed down to the battalion level, is planned to fill this very need.) With a better ability to see, the 3-69th would have instantly understood its situation and therefore been able to expect the arrival of Iraqi forces and to then decisively engage them.

Company C/1-2 Marines

The Marines were in need of warning and targeting of enemy ground forces in and around Nasiriyah. Marine headquarters at the battalion, regimental, or Marine Expeditionary Brigade/MEF level might have helped by providing voice warning or by placing red force location indicators on company or platoon situation awareness tools (for example, BFT). Targeting of the Iraqi mortar units might have come from an orbiting UAS via a direct downlink to one or more of these higher headquarters. When Marine vehicles were disabled in Nasiriyah, onboard systems (for example, BFT) could have sent an immediate Mayday call, and the command elements conducting electronic overwatch would have known to send reinforcements immediately.

Had the Marines and CAS aircraft been able to see and understand blue and red force positions, in all likelihood blue-on-blue fratricide would have been prevented by providing the location of blue units to CAS aircraft and directing blue aircraft to red forces. It would also have helped to provide early ground and air support to other units engaged by enemy forces, such as the 507th Maintenance Company.

507th Maintenance Company

Today, the 507th would have been equipped with BFT to navigate so as to avoid contact in Nasiriyah. It would also have received a warning on its BFT from other units about enemy forces in Nasiriyah. Had it still been engaged, it would have been able to send an immediate troops-in-contact alert to request help. Of course, the ability to finish decisively would have remained dependent on the ability to perform immediate action drills and manage a firefight effectively—activities for which a robust network is helpful but at the margin.

Perhaps more important, the 507th's parent unit would have been better informed in planning the tactical movement during which the 507th was attacked. For example, the 32nd Army Air and Missile Defense Command could have accessed the 3rd Army movement plan to see which tactical units would be adjacent to the 507th and synchronized movement with the combat units in a position to provide support if enemy forces appeared. The same higher headquarters would have been in a position to overwatch the progress of the 507th, to provide warning if theater intelligence assets received a report of enemy activities in Nasiriyah, and to help avoid navigation errors. If an enemy did attack, the overwatch headquarters could have received a troops-in-contact alert and then requested support from the combat units with which they had previously synchronized tactical movement.

2/4/617th MP Company

The 2/4/617th MP Company and the convoys that it protected would have been helped by better synchronizing their operations. For example, it would have been helpful if the MPs had advance knowledge that the convoys would be operating in the company's area that day, their expected time of arrival in the AO, the radio frequencies in use by the convoy and escorts, the convoy commander's call sign, and so on. The MPs might have then had the opportunity to help the convoy's parent units adjust their plans to minimize the convoy's vulnerability to ambush. Doing so during the planning phase of operations might have included helping to identify potential trouble spots, planning routes to avoid them, and preventing the two convoys from meeting in front of potential ambush sites.

In its electronic overwatch role, the company headquarters might also have obtained advance warning of insurgent forces at the ambush point; for example, from unattended ground sensors, a UAV or rotary-wing reconnaissance aircraft, or a combat patrol just ahead of the convoys. The MP company would then have then have had the option to organize an attack against the insurgent forces and reroute the convoy or delay it until the insurgent forces were cleared.

2/C/1-24th Infantry

Better warning of potential insurgent attacks would have helped the 1-24th soldiers. It is possible that some Iraqi civilians had prior indications that an attack would take place against the 2nd Platoon combat outpost. A particularly good form of warning would have been a tip from Iraqi civilians that an attack was about to be mounted or was in progress. Alternatively, observations by Company C that Iraqi civilians were avoiding the area could have provided better tactical warning. Finally, the 1-24th could have temporarily forbidden traffic on the road that approached its combat outposts.

Alternatively, unattended ground sensors monitored by company or battalion headquarters acting in an overwatch role would have provided tactical warning of approaching truck traffic. Once the VBIED was spotted, the 2/C/1-24th's soldiers would have been better able to destroy the truck at a distance and protect themselves.

1-3rd SFG

The 1-3rd SFG soldiers would have benefited from advance knowledge of insurgent heavy weapons positions in caves overlooking Syahcow (for example, from UAV reconnaissance). In addition, better surveillance of Syahcow would have helped to spot and track fleeing Taliban leaders.

Summary of Potential Network-Enabled Improvements

In summary, self-synchronization and electronic overwatch might have enabled forces at battalion and below levels to see first, understand first, act first, and finish decisively, as shown in Table 8.1.

Specifically, better networks might have improved the ability of

- tactical units to gain and maintain situational awareness of their own position, other friendly forces, and enemy forces
- tactical units and headquarters to better understand the current activities of friendly and enemy forces
- headquarters to better synchronize plans with units that they expected to be in proximity to their subordinate echelons

Table 8.1
Potential for Networks to Improve Unit Awareness and Synchronization in Historical Cases

	Unit						
Component	507th	C/1-2nd	3-69th	2/4/ 617th MP	2/C/ 1-24th Stryker	1-3rd SFG	Manned/ UAS Teams
See first							
Understand first							
Act first							
Finish decisively							

- tactical units to synchronize situational awareness and operations with other U.S. ground and air forces
- U.S. and coalition forces to act first, including to prevent or preempt enemy actions
- tactical units to react to tactical surprises and defeat the enemy, including a better ability to replan maneuver and fires.

Potential DOTMLPF Changes to Improve Networks

Doctrine

Army doctrine needs to enable leading-edge elements to see first, understand first, act first, and finish decisively. Accomplishing this "network dominance" becomes more difficult at the leading edge as enemies avoid presenting themselves en masse as regular combat forces. It also becomes more difficult as the leading edge of operations is assigned to smaller and lower-echelon units. Lower-echelon units will require help from the network when operating at the leading edge against forces hiding in urban terrain or among the population.

This help can come directly from adjacent units operating in proximity, so long as these adjacent units can synchronize their information, plans, and capabilities. For this to work, doctrine will need to

allow and even encourage adjacent units to self-synchronize while still maintaining their primary obligation to follow their orders.

Help can also come from higher-echelon forces when those higher echelons take on the duty of providing electronic overwatch of units operating forward. Overwatch can be provided by a unit's own higher headquarters. In some cases, an overwatch duty might be assigned to an adjacent unit when it is in a tactical situation that allows it to successfully serve in this role.

Organization

Self-synchronization of adjacent units will require a new concept of organization that enables units in close proximity or moving toward each other to provide close mutual support. Self-synchronizing units will need a fair degree of flexibility to adjust their maneuver and fires plans to provide support as the tactical situation evolves, and they will need rapid access to communication information (for example, command frequencies, call signs, and crypto keys) to allow them to hail nearby units and effect the appropriate coordination and cooperation.

Electronic overwatch duties can be assumed by higher-echelon headquarters or can be assigned to adjacent headquarters or command posts. This concept requires that the headquarters or command posts assuming this duty have the appropriate staff, the network tools, and the training needed to perform the required tasks.

Training

Soldiers and leaders will require specialized training to use the network in a self-synchronizing or electronic overwatch fashion. Some of this training is available today, but much of it is informal and it is a happy coincidence that soldiers use the same informal systems in theater that they used in garrison. Training will be needed to implement the concepts purposely built for such activities as self-synchronization and electronic overwatch.

Materiel

The hardware, software, and databases needed to conduct self-synchronization or electronic overwatch include the following.

SIPRNet. SIPRNet (or a similar classified, Web-based network) is needed to build databases and the tools to find, access, display, and use these data. At present, SIPRNet is available to corps and division headquarters on the move and to brigade and battalion headquarters on a permanent halt. Company command posts, when not colocated with higher headquarters, have historically not had access to SIPRNet—although they are now receiving access. This access may also be needed at the platoon level if these echelons continue to man combat outposts in the presence of enemy forces or conduct operations to identify insurgents.

Blue Force Location, Identification, Tracking, and Synchronization. The BFT system is available down to the squad and even individual vehicle level in maneuver units. Blue force tracking (generically) is needed in every unit that conducts independent operations. In part, this is because they may have to request reinforcements or fire support from parent units or units that happen to be in proximity and able to help.

Voice and Text Communication. Voice communication is needed between units operating independently and their sources of support. Text communication is also important to enable synchronization between units moving near one another. These forms of communication are among the most valued by forward echelons.

Intelligence, Surveillance, and Reconnaissance Systems. Units need the ability to receive ISR data from a variety of sources in their operating areas. RSTA units can provide some of this. As we have discussed, appropriately equipped scouts on patrol are an important source of ISR information. Stationary sensors and combat aircraft are also important sources of ISR information. One of the most useful sources in the most recent operations are the unmanned air systems used by all of the services. UASs can provide important capabilities for units in major combat operations and COIN operations. These capabilities can be put to direct use when ground units can control and downlink imagery directly from these UASs. Important, but more limited, information can be provided by direct downlink from UASs flying over an area but not under the control of proximate ground forces. Finally, some important information, such as red force alerts, can be provided

to units in the field via electronic overwatch conducted by higher echelons or specially organized overwatch elements.

Leadership and Personnel

Soldiers and leaders use both real-time battlefield information, as described above, and other sources of information for "background" or "foundational" knowledge. For example, soldiers use sites such as CompanyCommand Forum as a place to meet, learn, and build new concepts. This includes meeting current company commanders with whom they can share ideas about their profession of arms. They can also meet current and former commanders with experience in the same theater (such as leading patrols in Iraq or Afghanistan) or with relevant recent experiences (such as commanding an armored company or dealing with the death of a soldier killed in action). These experiences can help soldiers better deal with difficult situations and build standard operating procedures for their own units.

Once in theater, soldiers can use similar sites, such as the secure military forum CavNet, to share information and experiences with their peers, superiors, and subordinates. Sites located on SIPRNet can tap into a multitude of classified databases to gather intelligence concerning recent enemy movements, attacks, and other activities. Intelligence databases can contain HUMINT data, biometrics, and other information to help in the identification, surveillance, and tracking of known or suspected terrorists or guerrillas. In fact, there have been complaints from senior commanders that there are too many of these databases, that they are not compatible with each other, and that the information in them is not consistent.[9]

However, some soldiers have built new applications that enable them to use these databases in novel ways. For example, the Artillery Portal allows soldiers and leaders to display recent insurgent rocket and mortar attacks in Iraq to predict where future attacks might be staged. Similar tools have been developed to find patterns in insurgent behavior that may help to predict future attacks.

[9] Vines (2006a).

CHAPTER NINE

The Military Utility of Network-Enabled Operations: Conclusions and Recommendations

This chapter presents the top-level conclusions of this study as distilled from the observations given at the end of the individual chapters. The final section of this chapter offers the research team's recommendations, which tend to be actions that the G-6, G-3, and, in some cases, the G-2 would take the lead in implementing, given their respective roles in network technology, battle command, and intelligence and information management.

Conclusions

The analyses presented in this monograph lead to the following conclusions.

Army Networks Enabled the "Quality of Firsts" for Senior Army Tactical Echelons During Major Combat Operations

The ability of U.S. forces to gather, process, and disseminate battlespace information in a networked fashion has given them a tremendous advantage in MCOs. This dominant battlespace information has allowed U.S. forces to move faster and apply military power more aggressively and more effectively than U.S. adversaries. Today's networks enable several key operational capabilities:

- shared situational awareness of U.S. forces, although a current or complete red picture was sometimes not available to echelons below brigade

- unity of action between U.S. forces
  - superior coordination and synchronization of U.S. forces when on the offensive—that is, when they have the initiative
  - promising instances of excellent coordination and synchronization when reacting to enemy actions or attacks
- enhanced shared understanding.

The most significant problem noted during past MCOs was an incomplete or outdated view of red forces. New investments, such as UAS and the DCGS-A, may help to improve the red force information available to lower echelons.

Army Networks Have Not Yet Enabled the Same "Quality of Firsts" for SSTR, COIN, and Irregular Warfare Operations

Today's networks do not yet enable all of the force-enhancing effects that the Army expects. Army units often do not see first or act first when enemies use irregular tactics:

- Many reconnaissance, surveillance, and information systems were developed to find conventional armies when U.S. forces have the initiative.
- They are less effective in detecting and identifying irregular enemies before they initiate attacks.
- Information superiority in COIN and irregular warfare can therefore shift from U.S. forces to insurgents.

The Army's current networks do not yet enable seeing first or understanding first in all SSTR, COIN, and irregular warfare operations. The networks enable situational awareness of other blue units but do not always provide reliable awareness of red units before they attack, which is much more challenging. The networks do generally support reactive tactical coordination and unity of action, thereby usually allowing units to finish decisively.

Soldiers and Leaders Are Informally Linking Networks Together to Enhance Their Effectiveness

Our officer survey data revealed the following:

- Informal networks—often hosted on SIPRNet—received the highest ratings of all the networks.
- SIPRNet was rated as better than the other systems at establishing shared situational awareness with U.S. forces.
- Key systems—for example, SIPRNet and CPOF—are often not available at the company level and below—echelons that increasingly operate independently.

The SIPRNet was noted by the officers we surveyed as the best tool for establishing situational awareness between U.S. units. Where available, the SIPRNet was an essential means of connecting soldiers and leaders with sensitive databases and other sources of information within theater or elsewhere in the world. Unfortunately the SIPRNet and other widely used tools such as FBCB2 and CPOF are not typically shared with coalition or host-nation units.

The case studies and surveys we conducted reveal that soldiers and leaders are investing time and unit resources in informal networks that connect and fill gaps in the formal networks. These include unit-level databases to gather information from (and for) local operations; user applications to sort, search, and make sense of these data (i.e., cognitive aids); and social networks to share this knowledge with peers brigade-, division-, and corps-wide. The blogs, online discussion groups, and chat-rooms prompted by such shared application spawn an important "social domain" of the network to enhance the effectiveness of unit-, task-force-, or theater-wide operations.

Opportunities Are Emerging for the Army to Enhance Future Operations

The case studies and surveys we conducted reveal that soldiers and leaders are investing time and unit resources in informal networks that connect and fill gaps in the formal networks. These include unit-level databases to gather information from (and for) local operations;

user applications to sort, search, and make sense of these data (that is, cognitive aids); and social networks to share this knowledge with peers brigade-, division-, and corps-wide. The blogs, online discussion groups, and chat rooms prompted by such shared applications spawn an important "social domain" of the network to enhance the effectiveness of unit, task-force, and theaterwide operations.[1]

We saw significant potential to enhance the effectiveness of U.S. and coalition forces by providing networks that can enable

- adjacent U.S. units to self-synchronize
- command posts and higher headquarters to provide "electronic overwatch."

As noted in this monograph, ground forces are putting more and more information onto SIPRNet, FBCB2, CPOF, and other networks that can be used to synchronize the operations of adjacent units and units that are moving adjacent to each other. Often, this information can be updated automatically, without placing additional obligations on already overtaxed command post staffs. For example, the movement tickets that convoys are supposed to generate before departure could be pushed automatically to the headquarters of each AO through which a convoy will move. These trip tickets, along with information broadcast en route over SLANT reports, would provide a way to synchronize the convoy with those forces it will move adjacent to. Similarly, any moving air or ground unit could synchronize its activities with other U.S. forces that it approaches in the battlespace.

Additional advantages may be gained when networks enable electronic overwatch. Command posts that are synchronized with lower-echelon forces in their areas of operation may be in the best position to provide support (such as intelligence, fire support, or even a quick-reaction force) to these forces when they most need it. Having the nec-

[1] The Army must develop its social domains further. The Army needs to and will embrace Web 2.0 technologies (e.g., Facebook, MySpace, WIKIs, and blogs) and other social domains. The soldiers of today use these technologies in civilian life, and the Army needs to make them available on the battlefield of today. (Personal communication with Robert Landry, CIO/G6, February 11, 2009.)

essary connections, tools, knowledge, and mindset may allow these command posts to enhance the effectiveness of these units at critical moments.

Recommendations

The Army has made substantial investments in the network with the intention of achieving network-enabled operations. Indeed the rubric "see first, understand first, act first, and finish decisively" has become pervasive in current and future concepts. Assuming that the Army continues to believe that the network and network-enabled operations can deliver enhanced battlefield performance, we recommend that the Army pursue the network objectives described below.

Continue and Expand Efforts to Extend the Network to Lower Echelons

Out at the tip of the spear, small units experience limited network access and capabilities. Often, platoons and squads are operating on the move or in combat outposts far from other units and lack direct access to intelligence, surveillance, and reconnaissance data. Current plans to distribute UAVs downward through the brigade combat teams are a step in the right direction, along with direct-downlink terminals. In addition, providing the DCGS-A down to battalion and company levels will help. The key future challenge will be maintaining these connections to units on the move and building display systems that enhance effectiveness during high-intensity operations. More recent initiatives to provide Human Terrain Teams, Cryptologic Support Teams, and other specialized support at echelons brigade and below should be continued.

Many of the officers who responded to the project's surveys called for forward distribution of a SIPRNet-like Web-based classified system to lower-echelon units. SIPRNet is now reaching some company-level units at fixed sites, but platoons are increasingly assigned to man remote outposts. Where appropriate, the Army should develop the means to provide secret channels down to the lowest level of isolated

units. Where this is not possible (because of operational security concerns, limited bandwidth, and so forth), higher headquarters should provide electronic overwatch.[2]

One aspect of extending the network should be to extend its capabilities to identify the enemy before the shooting starts. The Army should intensify its efforts to expand its reconnaissance tools. In addition to the efforts under way, the Army might also consider emblematics, more biometrics, and new ways of instrumenting the battlespace that would reveal enemy combatants and their organizations. Another aspect of extending the network would be to take advantage of current ISR "feeds" by distributing them down the chain of command to smaller units that could use this information as context for understanding the clues they are collecting about the enemy within their own area of operations.[3]

Invest More Time in Developing and Exploiting Informal Networks

Officer survey responses indicate that informal networks perform important functions within and among deployed units. It appears that they may fill gaps in information and connectivity not provided by the formal network. The Army has supported some of these soldier initiatives—and should strive to study and harness these networks as they emerge. The G-6 and G-3 will want to coordinate closely to begin thinking about how to manage the intersection of systems of record with informal networking practices and how insights from such a process might inform network design and battle command practices.

Expand the Network to Include All Important Actors

A central tenet of irregular warfare is that the military provides only part of the solution. The host nation, coalition partners, other U.S. executive-branch agencies (such as the U.S. Department of State and the U.S. Agency for International Development), international agencies,

---

[2] This is a long-range Army CIO/G-6 goal, but funding and bandwidth are limitations.

[3] There will always be a "lack of connectivity" from the outer edges of the network. Soldiers at the team, squad, platoon, and company level move faster than their connectivity. Wideband connectivity below battalion level has not yet received priority for funding.

and nongovernmental organizations must be included. Expanding the network to include such a wide range of other actors clearly presents issues about operational and information security, but there are some precedents for handling them. CENTRIX, despite its limitations, suggests one way to undertake extended connectivity and share "rapid-decay" current intelligence, since it makes enemy exploitation of leaked intelligence difficult. This would also promote unity of effort and good faith with any number of participants.

Still, some nations, NGOs, and individuals may require extensive vetting over considerable periods of time. It may be necessary to continue the Special Forces practice of using unclassified, commercial radios and computers to connect these groups and individuals with U.S. forces—recognizing that these communications are very likely to be intercepted.

Enact DOTMLPF Changes to Enable Self-Synchronization and Electronic Overwatch

Some changes to Doctrine, Organization, Training, Materiel, Leadership, and Personnel may also be indicated.

- Doctrine
  - Platoons and squads need help when operating alone against irregular or hidden forces. Doctrine needs to allow and encourage adjacent units to self-synchronize information, plans, and capabilities while executing their assigned missions.
  - Overwatch duty might be assigned to an adjacent unit when it is in a tactical situation that allows it to provide support.
- Organization
  - Provide designated headquarters and command posts with the appropriate staff, network tools, and training needed to conduct electronic overwatch.
- Training
  - Provide training to implement self-synchronization and electronic overwatch.
- Materiel

  - *SIPRNet:* Provide SIPRNet down to the platoon level if these echelons continue to man combat outposts.
  - *Blue force location, identification, tracking, and synchronization:* Provide real-time blue force tracking to every unit that conducts independent operations. (Also, provide the best red picture possible on this equipment.)
  - *Intelligence, surveillance, and reconnaissance systems:* Continue to provide organic ways to access intelligence, such as direct UAS downlinks and DCGS-A. Enable electronic overwatch over voice and text systems for those echelons not able to receive DCGS-A.
- Leadership and Personnel
  - The Army leadership should encourage its soldiers and leaders to develop and use sites such as Companycommander.mil and CavNet as a place to meet, learn, and build new concepts.
  - The Army should also reward soldiers and leaders who develop new applications to tap into the multitude of classified databases to gather intelligence concerning recent enemy movements, attacks, and other activities.

APPENDIX A

Officer Impressions of Network Performance

Survey Development

The initial survey was developed as a short paper questionnaire to be filled out by selected Army officers. RAND team members administered these questionnaires during in-person visits to selected Army installations from January to March 2007. The goal of this initial effort was to obtain a broad overview of selected officers' views of network functionality. Capturing the breadth of officer experience with the network is a difficult task, because the network exists and operates in a great many forms (as discussed above) and individual experiences and interactions with the network may differ significantly.

To identify common themes in these diverse experiences, we decided to organize the survey around four basic constructs that the team identified as critical to overall network functionality: reliability, connectivity, content, and functionality. We define these constructs as follows:

- *Reliability* is a measure of how often the physical/information network is functional and available to the user when needed. If the network is either down or inaccessible by the user, its functionality is lost. The network is thus reliable if it meets both of these criteria most or all of the time when the user requires access.
- *Connectivity* examines whether the necessary linkages between different parties—commanders and subordinates, for example, or two or more habitually associated units—exist in the network and characterizes the quality of these connections. Rather than

address the reliability of the system as a whole, this construct focuses on the presence and reliability of key connections in the network. Connectivity exists within the physical and information domains (the technological connections must be in place for a connection to exist) but is also an important construct in the social network domain.

- *Content* measures the usefulness, accuracy, and timeliness of the information passed over the network. Although the network itself is not necessarily responsible for generating this content, it should be able to deliver the correct information to the end user at the time needed. Ultimately, information passed over the Army's network is used to make difficult decisions in real time, and this construct also speaks to how useful and central the information passed is to making these decisions.
- *Functionality* encompasses several related measures: the network's adaptivity to different physical environments; its ability to collect, organize, and process data; and its overall capacity to provide value-added to Army commanders. These measures together address the network's ability to enable true understanding and situational awareness, regardless of the circumstances (for example, whether stationary or on the move).

To develop the survey, we asked one or more questions from each construct for four broadly defined formal network types: command, sustainment, fire support, and intelligence networks. Rather than address a specific networking system (such as FBCB2 or SIPRNet), each network type encompasses multiple systems of record. We addressed the questions at this level to obtain broad impressions and experiences rather than narrow, less-comparable critiques. Some officers reported difficulty responding at this level of generality, and we used these concerns in developing the subsequent Web-based survey. Nevertheless, we felt that the simple, overview approach was appropriate for the exploratory nature of the survey. These questions used a five-point scale of frequency (ranging from "none of the time" to "all of the time").

In addition to the construct-specific questions, we also asked participants to provide overall ratings of each of the four network types, on a 1-to-5 scale (poor to excellent). Finally, the officers were asked if they had any other comments about that specific network type and were provided with space for written responses.

The last portion of the survey asked officers about their experiences with "informal," Internet protocol (IP)–based network tools, such as chat software, commercially available VoIP, mapping programs such as Google Earth, and so on. These questions were designed as a series of statements about the use of such informal networks, with which the officer could agree or disagree using a scale of 1 to 5 (false, rarely true, sometimes true, often true, entirely true). The questions were designed to mirror the construct-based questions above and elicit the reliability, connectivity, content, and functionality available via these informal paths that may or may not be available through formal systems. The survey also asked how often the participant uses informal networks, once again requesting an overall rating of this network type, and provided space for the officers to include additional written responses about the informal network tools they use.

Survey Population

The initial survey was designed to capture the impressions of a small sample of officers, and we therefore performed no representative sampling for this iteration. Instead, we identified and sought the impressions of a purposely biased sample of officers and sent RAND team members to each location to administer the survey. The selected locations included the Army War College, Fort Benning, Fort Sill, and Fort Leavenworth. We sought the impressions of War College students because they would have been battalion commanders or senior staff officers during their overseas assignments. We likewise sought students at the Intermediate Level Education course (formerly the Command and General Staff College) and the School of Advanced Military Studies at Fort Leavenworth because their impressions of network performance would have been formed during their tenures as company commanders and battalion-level staff officers. Finally, we administered the

survey at Fort Benning and Fort Sill to capture the impressions of more junior officers in the advanced courses at the Infantry and Field Artillery schools, whose overseas experience would have been as platoon leaders and in similar company-grade jobs. Participants at each location volunteered their time to complete the survey. Because we chose a deliberately biased convenience sample, the responses from this survey are not representative of the impressions of the officer population as a whole.

Data Collection

RAND staff visited the Army installations on the following dates:

- Army War College, January 25, 2007
- Fort Sill, February 20–21, 2007
- Fort Leavenworth, April 16–18, 2007
- Fort Benning, February 5–6, 2007.

The surveys were administered by RAND staff and written responses were provided by volunteering officers. During each visit, RAND team members introduced the survey, provided an overview briefing to each volunteer, and answered questions as needed during the written portion. Some participants also stayed after completing the survey and participated in an informal discussion of network functionality with RAND personnel. In addition, several other officers heard about the survey by word of mouth and voluntarily submitted paper questionnaires via mail or email. Respondents were asked for their rank and military occupational specialty (MOS), but no names or other personal data were recorded on the paper questionnaires to preserve response anonymity.

Data Analysis

Entry and Verification

RAND staff performed data entry from the paper surveys once they were collected and returned. Microsoft® Access® was used to store and manage the data, and responses were input directly into Access. To provide quality assurance for data entry, a separate team member randomly selected 20 of the 118 completed surveys and reviewed the electronic file for any entry errors or typos. No coding errors were detected during this review.

Summary Statistics

All statistical computations were completed using Stata statistical software. For each multiple-choice question, we generated tabulated results, simple means, and 95 percent confidence intervals. We also ran correlations to detect patterns between questions about specific system types or constructs, examined whether responses differed by rank or MOS, and performed a series of hypothesis tests to determine whether any of the overall system ratings were significantly different at the 95 percent significance level.

Written Responses

Written responses were examined separately for patterns by two members of the RAND team. We developed categories for the written responses and binned them appropriately using an informal consensus approach. The written comments were also used to inform the development of the second, Web-based survey.

Survey Instrument

The original paper questionnaire is provided below.

U.S. Army G-6 Network Functionality Survey

The Army's Chief Information Officer/G-6 is sponsoring this study to examine tactical network functionality. By completing this short survey, you are contributing to the G-6's understanding of current Army networks and their operations. Thanks for your help.

Please rate the networks with which you have personal experience. Rate their usefulness from your own point of view at the time you were using them, for example as a platoon leader/platoon sergeant, company executive officer, company commander, operations sergeant, battalion staff officer, command sergeant major, or battalion commander.

Your grade or rank _____

Branch/MOS _____

(Check All That Apply)

Overseas experience: 1☐ Afghanistan 2☐ Iraq 3☐ Bosnia 4☐ Kosovo

Rating attributes of networks. Just check the box below the phrase that most closely describes your experience. For example, answering question 1a below, if you found the command net was always up when you needed it, you would place a checkmark in the box below the phrase, "All of the time"

1. Command Net (voice, digital, IP-based, other):

(Check One Box on Each Line)

	All of the time	Most of the time	Half of the time	Some of the time	None of the time
a. **Reliability**: was it up when you needed it?	1☐	2☐	3☐	4☐	5☐
b. **Connectivity**: could you reliably reach your subordinate units?	1☐	2☐	3☐	4☐	5☐
c. **Connectivity**: could you reliably reach your next higher?	1☐	2☐	3☐	4☐	5☐
d. **Content**: did you get useful instructions/information over this net?	1☐	2☐	3☐	4☐	5☐
e. **Content**: was information on this network timely?	1☐	2☐	3☐	4☐	5☐
f. **Content**: was information on this network accurate?	1☐	2☐	3☐	4☐	5☐
g. **Content**: did net information support sound decision-making?	1☐	2☐	3☐	4☐	5☐
h. **Functionality**: did the network perform well on the move?	1☐	2☐	3☐	4☐	5☐
i. **Functionality**: did the network perform well once stationary?	1☐	2☐	3☐	4☐	5☐
j. **Functionality**: did the net support coordination with units on your flanks?	1☐	2☐	3☐	4☐	5☐
k. **Functionality**: did the network contribute to good situational awareness?	1☐	2☐	3☐	4☐	5☐
l. **Functionality**: did the network enable sound maneuver?	1☐	2☐	3☐	4☐	5☐

(Continued)

1. Command Net (voice, digital, IP-based, other):

m. **What else** (content, function) would you like on this network (please specify voice, digital, etc. as the basis for your comments)?

_____

_____

_____

_____

n. **Overall rating for the command net:**

(Check One Box)

1☐ Excellent 2☐ Very good 3☐ Good 4☐ Fair 5☐ Poor

2. Sustainment Net (voice, digital, IP-based, other):

(Check One Box on Each Line)

	All of the time	**Most of the time**	**Half of the time**	**Some of the time**	**None of the time**
a. **Reliability**: was it up when you needed it?	1☐	2☐	3☐	4☐	5☐
b. **Connectivity**: did the net link you with all your critical combat service support providers (or, if you work in sustainment, did it link you to your consumers)?	1☐	2☐	3☐	4☐	5☐
c. **Content**: did useful information pass over this net?	1☐	2☐	3☐	4☐	5☐
d. **Content**: was this information timely?	1☐	2☐	3☐	4☐	5☐
e. **Content**: did net information support sound decision-making?	1☐	2☐	3☐	4☐	5☐
f. **Functionality**: did the network perform well on the move?	1☐	2☐	3☐	4☐	5☐
g. **Functionality**: did the network perform well once stationary?	1☐	2☐	3☐	4☐	5☐
h. **Functionality**: did the network enable robust sustainment?	1☐	2☐	3☐	4☐	5☐

i. **What else** (content, function) would you like on this network (please specify voice, digital, etc. as the basis for your comments)?

_____

_____

_____

_____

j. **Overall rating for the sustainment net:**

(Check One Box)

1☐ Excellent 2☐ Very good 3☐ Good 4☐ Fair 5☐ Poor

3. Fire Support Net (voice, digital, IP-based, other):

(Check One Box on Each Line)

	All of the time	Most of the time	Half of the time	Some of the time	None of the time
a. **Reliability**: was it up when you needed it?	1☐	2☐	3☐	4☐	5☐
b. **Connectivity**: did the net link you with all your organic fire support assets?	1☐	2☐	3☐	4☐	5☐
c. **Connectivity**: did the net link you with all the available non-organic fire support assets?	1☐	2☐	3☐	4☐	5☐
d. **Content**: was this information on this network timely?	1☐	2☐	3☐	4☐	5☐
e. **Content**: was the information on this network accurate?	1☐	2☐	3☐	4☐	5☐
f. **Content**: did net information support sound decision-making?	1☐	2☐	3☐	4☐	5☐
g. **Functionality**: did the network perform well on the move?	1☐	2☐	3☐	4☐	5☐
h. **Functionality**: did the network perform well once stationary?	1☐	2☐	3☐	4☐	5☐
i. **Functionality**: did the network deliver timely, accurate fire support?	1☐	2☐	3☐	4☐	5☐

j. **What else** (content, function) would you like on this network (please specify voice, digital, etc. as the basis for your comments)?

_____

_____

_____

_____

k. **Overall rating for the fire support net:**

(Check One Box)

1☐ Excellent 2☐ Very good 3☐ Good 4☐ Fair 5☐ Poor

4. Intelligence Net:

(Check One Box on Each Line)

	All of the time	Most of the time	Half of the time	Some of the time	None of the time
a. **Reliability**: was it up when you needed it?	1☐	2☐	3☐	4☐	5☐
b. **Connectivity**: did the net link you to all critical intelligence/information sources (UAVs, UGS, radars, observers, etc.)?	1☐	2☐	3☐	4☐	5☐
c. **Content**: was this information on this net timely/accurate/reliable (e.g., targeting quality)?	1☐	2☐	3☐	4☐	5☐
d. **Content**: did the information support sound decision-making?	1☐	2☐	3☐	4☐	5☐
e. **Functionality**: did the network perform well on the move?	1☐	2☐	3☐	4☐	5☐
f. **Functionality**: did the network perform well once stationary?	1☐	2☐	3☐	4☐	5☐

g. **What else** (content, function) would you like on this network?

_____

_____

_____

_____

h. **Overall rating for the intelligence net:**

(Check One Box)

1☐ Excellent 2☐ Very good 3☐ Good 4☐ Fair 5☐ Poor

5. Informal Networks (e.g., IP-based networks that emerge to help a given community of soldiers: Outlook, chat rooms, etc.)

(Check One Box on Each Line)

These statements are…	**Entirely true**	**Often true**	**Sometimes true**	**Rarely true**	**False**
a. I relied on informal networks to get information more easily than through formal networks	1☐	2☐	3☐	4☐	5☐
b. I used informal networks because they offered ease of connectivity unavailable through official networks	1☐	2☐	3☐	4☐	5☐
c. I used informal networks and their tools because they offered functionality not available on official networks.	1☐	2☐	3☐	4☐	5☐
d. Informal networks made doing my job easier	1☐	2☐	3☐	4☐	5☐
e. I used informal networks solely for entertainment and staying in touch with friends	1☐	2☐	3☐	4☐	5☐
f. I rarely used informal networks	1☐	2☐	3☐	4☐	5☐

g. I used the following software applications and systems to help do my job:

_____

_____

_____

_____

h. **Overall rating for the informal networks:**

(Check One Box)

1☐ Excellent 2☐ Very good 3☐ Good 4☐ Fair 5☐ Poor

Anything else you think the Army Chief Information Officer/G-6 should understand about the functionality, utility, and reliability of your tactical networks? Send us an e-mail about your concerns. The research team can be reached through jpeters@rand.org.

APPENDIX B

Officer Impressions of the Performance of Network Programs of Record

Survey Objective

The second G-6 Network Functionality Survey was designed to gather the opinions of active-duty, commissioned officers who used the network during recent deployments to Iraq or Afghanistan. The survey asked officers about the performance of the Army network and about their experiences with specific formal systems.

Sampling Design

For this survey, we selected a stratified random sample of officers from the population of active officers currently serving in the Army. The goal of such a formalized design is to make better inferences about an entire population based on sample results, in this case, the population of Army officers who have served in two significant theaters of combat since 2001. A detailed description of the sampling design is provided below.

Sample Frame and Eligibility

We used the Officer Master File (OMF) database provided by Headquarters, U.S. Department of the Army, to develop a suitable sampling frame for the population of interest. The OMF is a suitable list from which to sample because it covers the entire target population, contains no duplications, and provides sufficient demographic information to identify and contact the population of interest.

For this effort, we sought officers with in-theater experience using the Army network. Therefore, we restricted our sample to officers ranked first lieutenant through colonel (O-2 through O-6) and working in selected combat and combat support branches. Table B.1 shows the universe of officers in the desired ranks and branches according to the OMF database of May 2007.

We sought to collect opinions only from officers who were deployed to Iraq or Afghanistan between 2001 and the time of the survey. Because of incomplete deployment data in the OMF database, however, we were unable to develop a sample frame of only deployed officers in the desired ranks and branches and could not preselect for that criterion. Instead, we used a series of questions at the beginning of the Web survey to determine whether a respondent met the deployment requirements.

Strata Development

For this survey, we intended to make inferences about officers in the rank/branch subgroups listed in Table B.1 and thus stratified the sample on both rank and branch. For each group, we sought a precision of ±0.5 on a 1–5 Likert scale. Assuming a population standard deviation of 1.0 on the same scale, using standard sample size

Table B.1
Sample Frame of Officers in Selected Ranks and Branches

	Rank				
Branch	**O-2: 1LT**	**O-3: CPT**	**O-4: MAJ**	**O-5: LTC**	**O-6: COL**
Armor (AR)	520	1,138	919	527	196
Field Artillery (FA)	769	1,427	1,096	712	275
Infantry (INF)	1,013	1,903	1,369	902	417
Military Police (MP)	262	612	404	224	83
Ordnance (ORD)	424	989	666	446	157
Quartermaster (QM)	447	1,031	694	478	140
Signal (SIG)	738	1,418	784	515	173
Transportation (TRN)	456	857	465	288	112

calculations, this yielded a required minimum sample size of approximately 85 respondents.[1] Rounding up yielded a target response of 100 per subgroup. After examining previous surveys conducted at RAND, we estimated an overall response rate of 50 percent, which yielded a final sample size of 200 per stratum. Most subgroups became individual strata, and random samples of officers were generated.

However, six of the subcategories at the O-6 level are populated with fewer than 200 officers, according to the OMF. To ensure an appropriate sample, we merged these O-6 subgroups with their O-5 counterparts and randomly sampled 200 officers from this merged population. For instance, 83 colonels in the Military Police branch were merged with the 224 lieutenant colonels in the same branch, and 200 officers were sampled from this combination. The only exception was colonels in the Armor branch (196 officers). Because the size of this subgroup is approximately 200, we decided to send survey requests to every officer in the group. In total, we selected 6,996 officers to participate in the survey. Table B.2 shows the final strata and sample sizes for each stratum.

Table B.2
Final Strata and Sample Sizes

	Rank				
Branch	**O-2: 1LT**	**O-3: CPT**	**O-4: MAJ**	**O-5: LTC**	**O-6: COL**
AR	200	200	200	200	196
FA	200	200	200	200	200
INF	200	200	200	200	200
MP	200	200	200	200	200
ORD	200	200	200	200	
QM	200	200	200	200	
SIG	200	200	200	200	
TRN	200	200	200	200	

[1] Assumes a 0.05 confidence level and 0.90 power.

Sampling Weights

Because we stratified the sample of officers, those belonging to different subgroups had different underlying probabilities of selection. When aggregating across strata, then, sampling weights for each observation were required to correct for the selection probability differences. We also used these weights to adjust for nonresponse.

In a stratified random sampling design, the appropriate sampling weights are simply the reciprocal of the probability of selection within each stratum. Thus, the initial weight for the h^{th} stratum, V_h, is

$$V_h = \frac{N_h}{m_h}$$

where N_h is the total population of stratum h and m_h is the number of officers sampled from the stratum.

However, the initial weights assume a 100 percent response rate, so that everyone sampled in a stratum responded and was eligible for the survey. This was not the case for the G-6 survey, so the next step of the calculations is to apply a simple correction for nonrespondents and ineligible participants:

$$\delta_h = \frac{m_h}{n_h}$$

where δ_h is the correction factor for each stratum h, m_h is the number of officers sampled, and n_h is the number of eligible respondents in the stratum. Then, the final weights, w_h, are calculated as

$$w_h = V_h \delta_h$$

which can be rewritten as

$$w_h = \frac{N_h}{n_h}$$

for each stratum h.

Thus, the sampling weights used are simply the ratio of the total population and eligible response rate for each stratum.[2] As the number of eligible respondents increases, the stratum weight declines, because each respondent represents fewer members of the stratum population. For the stratum we sampled with certainty (as a census), each respondent received a weight of one. Note that more complex weighting approaches that are better able to account for differences between respondents and nonrespondents, such as propensity weighting/scoring, were not possible because we lacked demographic information about the sample frame beyond rank and branch.

Poststratification for Formal System Responses

The third part of the survey asked officers to provide feedback on specific formal systems that they used while deployed (for example, CPOF and FBCB2). We were unable to predict how many responses we would receive about each system, however, and in many cases we received an insufficient number of responses to make use of the strata weights defined above (that is, some strata had zero responses or only one). To improve our mean estimates for the formal system responses, we therefore decided to poststratify at a higher level of aggregation. We developed these new strata by dividing the included ranks into two groups—battalion and below (O-2 through O-4) and echelons above battalion (O-5 and O-6). Branches were also placed in one of two bins: Combat (Infantry, Armor, and Field Artillery) and Combat Support (all remaining branches). This yielded four strata overall for poststratification. Weights were then developed for the new strata using the previously described method and applied to all summary estimates for the formal system responses. Table B.3 shows the poststratification categories and sample frame.

[2] These weights are less than ideal given our lack of knowledge of the number of eligible officers in the population. Better weights would use as the strata populations only those officers deployed to Iraq or Afghanistan from 2001 to the time of the survey. The current weights were used because this information was unavailable to the study team at the time of publication.

Table B.3
Formal System Strata Sample Frame

	Rank				
	Battalion and Below			Echelons Above Battalion	
Branch	O-2: 1LT	O-3: CPT	O-4: MAJ	O-5: LTC	O-6: COL
	Combat				
AR					
FA		10,154			3,029
INF					
	Combat Support				
MP					
ORD					
QM		10,247			2,616
SIG					
TRN					

NOTE: Numbers in the shaded cells denote total populations in each group.

Survey Development

Protocol Design

The survey protocol was designed based on the work of Evidence Based Research, Inc. (EBR) and the Network Centric Operations Conceptual Framework that EBR developed. The framework is composed of the four domains of the network: physical, information, cognitive, and social. Each domain is further resolved to discrete concepts, such as quality of individual information. The survey protocol was organized into five sections:

1. demographics (rank, branch, and deployment history)
2. quality of network and network devices
3. quality of formal and informal information

4. quality of formal systems, such as ABCS and CPOF
5. open response.

In the demographic section, we asked the officers for their rank, branch, number of times they have been deployed to various locations, and the time of their last deployment to Iraq or Afghanistan. The second section consisted of questions regarding connectivity, security, and capabilities of the communication network and network devices, such as phones, computers, and radios. The third set of questions pertained to the characteristics of formal and informal information, such as relevance, timeliness, and completeness. We then asked officers to choose from a list of formal systems with which they had significant experience. They were then asked to evaluate the system's performance in helping officers to share information, develop situational understanding, and make decisions. The same set of questions was asked for every system that they chose. Finally, we gave the officers an opportunity to respond openly about the Army's network. We asked them, "What else would you like to tell the CIO [Chief Information Officer]/G6 about the Army Network?" The survey protocol can be found in Appendix A.

Pretesting

The survey was pretested on a group of officers at the School of Advanced Military Studies (Command and General Staff College at Fort Leavenworth). Paper copies of the survey were administered to 21 officers. In addition to having them answer the survey questions, we also asked them to critique the questions. We took this opportunity to assess the average time required for the officers to complete the survey. After reviewing the officers' feedback, we added, deleted, and edited questions. We also asked the officers to write down the names of all the formal systems that they had significant experience using. Their responses helped us to generate a list of formal systems.

Internet Survey Programming

Recent guidance on survey design suggested that our study was a good candidate for conducting an Internet survey instead of a mail or in-person survey for the following reasons:[3]

- The survey was conducted in an organization that has a list of email addresses for the target population.
- The target population represented a small slice of the total population.
- The sample size was moderately large.
- The survey contained an important open-ended question. There is some evidence that respondents give longer answers to open-ended questions in electronic surveys than in printed surveys.

Following good Web survey design practice, we adhered to the following practices:

- listed only a few questions per screen
- eliminated unnecessary questions
- used graphics sparingly; this was especially important, since some of the officers may be using a slow connection in Iraq or Afghanistan
- reduced response errors by restricting response choices and by limiting fill-in answer options, using buttons and pull-down menus instead
- forced answers only on rare occasions
- made error or warning messages as specific as possible
- always password-protected the Web survey; this was important to ensuring that the officer's perception of privacy was maintained
- provided some indication of survey progress
- allowed respondents to interrupt and reenter the survey.

We also used the computer survey's capability to perform logic tests to prescreen respondents. After reviewing respondents' deploy-

[3] Schonlau, Fricker, and Elliott (2002).

ment locations and deployment dates, those ineligible were removed from the survey if they had not been deployed to Iraq or Afghanistan between 2000 and the time of the survey. Those who met that criterion were allowed to continue the survey.

One section of the survey investigates formal systems and asks officers to select from a list of those systems with which they have significant experience. To not overwhelm the respondents with a long list of systems, we streamlined the list based on the branch in which the officer worked (Table B.4). The systems were listed in order of importance for the study. However, note that respondents were also able to enter other system names and fill out the formal system questions for these customized entries.

Table B.4
List of Formal Systems, by Respondent's Branch

INF, AR, MP	TRN, ORD, QM	FA	SIG
FBCB2	BCS3	AFATDS	ISYSCON
CPOF	JDLM	JADOCS	FBCB2
MCS	MTS	FBCB2	CPOF
TAIS	CSS, VSAT	CPOF	MCS
AFATDS	ULLS	MCS	TAIS
JADOCS	FBCB2	TAIS	AFATDS
ISYSCON	CPOF	ISYSCON	JADOCS
SIPRNet	MCS	SIPRNet	SIPRNet
	TAIS		
	AFATDS		
	JADOCS		
	ISYSCON		
	SIPRNet		

NOTE: CSS = combat service support; VSAT = very small aperture terminal.

The electronic media also gave us the ability to track respondent behaviors, such as the time the survey was taken, the time taken to complete the survey, and even which Web browser was used to answer the survey questions.

We opted to store the survey on a RAND server to ensure easy access and control over the survey program in case technical problems arose or changes had to be made.

Data Collection

Distribution of Survey

Our project's action officer and other staff of the CIO/G-6 were invaluable in helping us obtain the email addresses of the selected officers. In an attempt to motivate high response rates from the officers, an email from the CIO/G-6 office was first sent to them. The email stated RAND's role in the study and the purpose of the survey and asked for the officers' participation. The day after the sponsor sent out the email, we followed with another email providing the link to the survey and assigning a unique username and password to each officer. We also provided a helpdesk phone number and email address to the officers. This email was sent to the first 1,000 officers, and we anticipated technical problems. However, we encountered no technical problems and the survey link was sent to the remaining 6,000 officers the following day.

The data-collection period began on August 9, 2007, and the Web survey was available to the officers for approximately one month (it was closed on September 10, 2007). During that month, up to three reminder emails were sent to officers who started the survey but did not finish as well as to those officers who had not started it:

Data Cleaning and Verification

Once data collection had ended, we made several modifications to the dataset before adding weights and generating results:

- The survey invitation had been erroneously sent to a sample of second lieutenants, and all respondents listed as 2LT in our sampling database were removed from the database as ineligible (270 total).
- Some respondents did not provide their rank or branch. In these cases, we imputed the necessary information from the OMF database to place these respondents in the appropriate strata (17 changes).
- Ninety-three respondents reported a different rank from that listed in OMF, and 35 reported a different branch. In these cases, the self-reported information was more accurate, so we accepted the changes and migrated these individuals into new strata (128 strata changes from the initial database).
- Some respondents manually entered formal systems that we considered to be part of a broader system of record (for example, Blue Force Tracker as a part of FBCB2). In these cases, we binned the manual entries into our definition of the formal system for ease of comparison.

Most changes were conducted in the Stata statistical software. Formal system data required further processing to develop separate entries for each system response. These changes were made using SAS® before converting the data back to Stata for analysis.

Response Rates

Out of 6,996 officers in the sample, 1,613 (23 percent) responded to the survey. After subtracting the number of respondents who were disqualified from the survey and addressing missing demographic fields and other strata changes (see the data-cleaning section, above), 1,036 eligible respondents remained (15 percent) (Tables B.5, B.6, and B.7).

Addressing Nonresponse

The eligible response rate of 15 percent fell considerably below the target rate of 50 percent. Because of the lower-than-expected response, we determined that we lacked sufficient statistical power to report

Table B.5
Response Rates for All Respondents and Eligible Respondents, by Rank

	All Respondents		Eligible Respondents	
Rank	No. of Officers	Percentage	No. of Officers	Percentage
O-2: 1LT	148	9.18	98	9.46
O-3: CAP	370	22.94	300	28.96
O-4: MAJ	419	25.98	252	24.32
O-5: LTC	414	25.67	240	23.17
O-6: COL	262	16.24	146	14.09
Total	1,613	100	1,036	100

NOTE: Percentages may not sum to 100 because of rounding.

Table B.6
Response Rates for All Respondents and Eligible Respondents, by Branch

	All Respondents		Eligible Respondents	
Branch	No. of Officers	Percentage	No. of Officers	Percentage
INF	221	13.7	147	14.19
AR	241	14.94	164	15.83
FA	259	16.06	162	15.64
MP	163	10.11	99	9.56
ORD	181	11.22	127	12.26
QM	155	9.61	98	9.46
SIG	246	15.25	154	14.86
TRN	147	9.11	85	8.2
Total	1,613	100	1,036	100

NOTE: Percentages may not sum to 100 because of rounding.

Table B.7
Percentage Response Rates, by Branch and Rank

	Rank				
Branch	**O-2: 1LT**	**O-3: CPT**	**O-4: MAJ**	**O-5: LTC**	**O-6: COL**
AR	6.0	17.5	13.0	19.5	17.5
FA	4.0	22.5	18.0	20.0	17.9
INF	6.0	20.5	16.0	19.0	19.5
MP	7.0	17.5	14.5	10.5	
ORD	5.5	20.5	14.0	23.5	
QM	5.5	14.5	15.0	14.0	
SIG	7.5	26.5	22.5	20.5	
TRN	7.5	10.5	13.0	11.5	

accurate, meaningful results at the strata (rank/branch subgroup) level. Instead, we decided to report results either in aggregate (to make inferences about the population of all eligible officers), by rank alone, or by branch alone. For the formal system responses, we reported results in aggregate or by using the poststratification categories described above.

Several factors likely diminished response rates. One, the database contained officers who had been retired for a few months, causing us to sample some retired officers. We received many emails from these retired officers declining to participate in the survey. Whether they had recent deployment experience or not, these officers seemed to perceive less obligation than active officers to complete the survey. As mentioned, many officers were disqualified because of their deployment history. Ironically, some were not able to connect to our survey because of heightened network security at their end; others reported that they were in theater and could not complete the survey because of a slow Internet connection. Finally, as shown in Table B.7, response rates for first lieutenants generally lagged behind those of other ranks. The reasons for this heightened nonresponse remain unclear, but these officers obviously have shorter deployment histories and may have self-selected out of the survey at the outset. It is interesting to note that we

received a few queries from officers not in our selected population but nevertheless eager to participate in it.

Our sampling and weighting methodologies assume that these nonrespondents are randomly distributed within each stratum. However, we were unable to test this assumption because of the lack of additional demographic information about respondents beyond rank and branch. The lower-than-expected response rates, coupled with our limited information about nonrespondents, may limit our ability to make population inferences using the collected data. Although the insights remain valuable, the reported results should be interpreted with some caution.

Survey Analysis

To generate the results presented in the main body of the monograph, we tabulated all results by question, calculated means and 95 percent confidence intervals in aggregate and for selected subgroups, checked for correlation between selected questions of interest, and performed a series of hypothesis tests to determine whether differences in response by subgroup were statistically significant. The mean and sample variance calculations took into account the sample weighting described above, whereas correlations were run unweighted. All calculations were performed in the Stata 8® statistical software.

Estimating Means

The means are estimated as simple weighted means, incorporating the previously defined probability weights. Stata defines the weighted mean estimator as a ratio with the denominator equal to the total population:

$$\hat{R} = \frac{\hat{Y}}{\hat{X}}$$

where

$$\hat{Y} = \sum_{h=1}^{L} \sum_{i=1}^{n_h} w_{hi} y_{hi}$$

is the weighted total of the answers to a given question (w_{hi} is the sampling weight and y_{hi} the response for individual i in strata h), and

$$\hat{X} = \sum_{h=1}^{L} \sum_{i=1}^{n_h} w_{hi}$$

is the sum of the weights, which equals the population total.

Plugging in, this yields the following mean estimator:

$$\hat{R} = \frac{\sum_{h=1}^{L} \sum_{i=1}^{n_h} w_{hi} y_{hi}}{\sum_{h=1}^{L} \sum_{i=1}^{n_h} w_{hi}}.$$

Estimating Sample Variance

The variance estimator was used to generate confidence intervals and hypothesis tests. Using the same definitions as above, Stata estimates weighted sample variance according to the expansion

$$\hat{V}(\hat{R}) = \frac{1}{\hat{X}^2}[\hat{V}(\hat{Y}) - 2\hat{R}\hat{C}ov(\hat{Y}, \hat{X}) + \hat{R}^2\hat{V}(\hat{X})].$$

We estimated sample variance with a finite population correction, which reduces the sample variance estimate as the size of the sample gets close to the population size. To generate the complete variance estimator with finite population correction, we first define the "residual" of the mean estimator as

$$d_{hi} = \frac{1}{\hat{X}}(y_{hi} - \hat{R}).$$

The weighted total for each residual is defined as

$$z_{dhi} = w_{hi} y_{hi}$$

and the corresponding weighted average is:

$$\bar{z}_{dh} = \sum_{i=1}^{n_h} z_{dhi}.$$

Then, the sample variance can be defined as

$$\hat{V}(\hat{R}) = \sum_{h=1}^{L} (1 - f_h) \frac{n_h}{n_h - 1} \sum_{i=1}^{n_h} (z_{dhi} - \bar{z}_{dh})^2$$

where $(1 - f_h)$ is the finite population correction, with $f_h = n_h/N_h$.[4]

[4] StataCorporation (2001).

(DRAFT) U.S. Army G-6 Network Functionality Survey (DRAFT)

The Army's Chief Information Officer/G-6 is sponsoring this study to examine tactical network functionality. By completing this short survey, you are contributing to the G-6's understanding of current Army networks and their operations. Thanks for your participation.

Your grade or rank _____

Branch _____

MOS _____

Number of deployments at each location:

Afghanistan _____ Iraq _____ Bosnia ____ Kosovo _____ Africa _____ Others

_____

Last time of deployment to Iraq/Afghanistan

(mm/yy to mm/yy) _____

Please answer the following questions in respect to your personal experience during your last deployment.

The survey is divided into 3 parts. The first part of the survey asks questions about the network and network devices. The second part asks about the information passed through the network. The last part of the survey asks questions about specific systems.

Part I : Quality of Network and Network Devices

Quality and degree of interconnections and network devices

A network is a system of interconnected nodes. Nodes can be all or a combination of people, computers, phones, radios, or other networking devices.

		Less than half of the time	**Half of the time**	**More than half of the time**	**All of the time**
How often could you reliably reach other units using voice (phone, radio, etc.)?					
subordinate units?	____	____	____	____	____
adjacent units?	____	____	____	____	____
higher units?	____	____	____	____	____

coalition units?	____	____	____	____	____
contractors/NGOs?	____	____	____	____	____
host nation military/police units?	____	____	____	____	____
How often could you reliably reach other units using text communication (email, mIRChat, etc.)?					
subordinate units?	____	____	____	____	____
adjacent units?	____	____	____	____	____
higher units?	____	____	____	____	____
coalition units?	____	____	____	____	____
contractors/NGOs?	____	____	____	____	____
host nation military/police units?	____	____	____	____	____
If your primary communication mode was not available, were alternate means available at the time that you needed them?	____	____	____	____	____
How often did the speed of the network significantly slow down your mission?	____	____	____	____	____
When your operational needs changed, did the network capabilities quickly change to meet your new needs?	____	____	____	____	____
Was the radio with the security type that you needed available when you needed it?	____	____	____	____	____
phone?	____	____	____	____	____
computer?	____	____	____	____	____
Was your operation affected by a limited number of radios?	____	____	____	____	____
phones?	____	____	____	____	____
computers?	____	____	____	____	____

Did the capabilities of the network device (such as durability, user-friendliness, battery life, etc.) slow down your work?	____	____	____	____	____

Part II: Formal and Informal Information

This section will ask about the quality of information. The questions are divided by information obtained from formal systems and information obtained from informal systems.

Formal systems are part of a program of record (e.g., all ABCS systems) or are systems that may not have a program of record but were mandated to be used by higher commanders (e.g., CPOF). Informal systems are ad-hoc systems, generally pushed bottom up (e.g.

Quality of Formal Information (Information that has been pushed or pulled using a formal information system such as ABCS systems, CPOF, etc.)	**None of the time**	**Less than half of the time**	**Half of the time**	**More than half of the time**	**All of the time**
How often were you able to obtain all the information that you needed to accomplish your task?	____	____	____	____	____
How often were you confident in the accuracy of the information obtained?	____	____	____	____	____
How often was the information obtained current enough to be useful?	____	____	____	____	____
How often did you understand all of the information that you needed to accomplish your task?	____	____	____	____	____
How often did information get pushed to you by other units?	____	____	____	____	____
How often did you push information to other units?	____	____	____	____	____
	None	**Less than half**	**Half**	**More than half**	**All**
Of all the information that was obtained, how much of it was useful?	____	____	____	____	____

Quality of Informal Information (Information that has been pushed or pulled using an informal information system such as mIRChat)	**None of the time**	**Less than half of the time**	**Half of the time**	**More than half of the time**	**All of the time**
How often were you able to obtain all the information that you needed to accomplish your task?	____	____	____	____	____
How often were you confident in the accuracy of the information obtained?	____	____	____	____	____
How often was the information obtained current enough to be useful?	____	____	____	____	____
How often did you understand all of the information that you needed to accomplish your task?	____	____	____	____	____
How often did information get pushed to you by other units?	____	____	____	____	____
How often did you push information to other units?	____	____	____	____	____
	None	**Less than half**	**Half**	**More than half**	**All**
Of all the information that was obtained, how much of it was useful?	____	____	____	____	____
Quality of Informal Network (IP-based networks that emerged to help a given community of soldiers such as mIRChat)	**None of the time**	**Less than half of the time**	**Half of the time**	**More than half of the time**	**All of the time**
How often did you rely on informal networks to get information more easily than through formal networks?	____	____	____	____	____
How often did you use informal networks because they offered ease of connectivity unavailable through formal networks?	____	____	____	____	____

How often did you use informal networks and their tools because they offered functionality not available on formal networks?	____	____	____	____	____
How often did informal networks make doing your job easier?	____	____	____	____	____
How often did you use informal networks solely for entertainment and staying in touch with friends and family?	____	____	____	____	____
How often did you use informal networks?	____	____	____	____	____

Part III: Quality of Formal Information Systems

The remainder of the survey asks about specific formal systems. You will be asked questions regarding the reliability, functionality, connectivity, and usability of the system. Please check all formal systems that you have had sufficient experience with

BCS3 (Battle Command Sustainment Support System)

JDLM (Joint Deployment Logistics Model)

MTS (Mobile Tracking System)

CSS VSAT (Combat Service Support Very Small Aperture Terminal)

ULLS (Unit Level Logistics System)

FBCB2 (Force Battle Command, Brigade and Below)

CPOF (Command Post of the Future)

MCS (Maneuver Control System)

TAIS (Tactical Airspace Integration System)

AFATDS (Adv Field Artillery Tactical Data System)

JADOCS (Joint Advance Deep Operations Coordination System)

ISYSCON (Integrated System Control)

Quality of <system name>

	Not at all	A little bit	Some-what	Quite a bit	Ex-tremely
How reliably did <fill in system name> facilitate sharing of information with other units?	____	____	____	____	____
with adjacent units?	____	____	____	____	____
with higher units?	____	____	____	____	____
with subordinate units?	____	____	____	____	____
with coalition units?	____	____	____	____	____
with host nation military/police units?	____	____	____	____	____
To what degree was the system user-friendly, i.e. had intuitive functioning, helpful manuals or smart cards?	____	____	____	____	____

Quality of Individual Sensemaking: Individual Understanding[1]	None of the time	Less than half of the time	Half of the time	More than half of the time	All of the time
How often did the <fill in system name> help you to understand the information more fully or deeply than you would have without using <fill in system name>?	____	____	____	____	____
How often did the <fill in system name> help you understand the information faster than you would have without using <fill in system name>?	____	____	____	____	____

	Ex-tremely im-portant	Very im-portant	Somewhat important	A little important	Not at all im-portant
How important was <fill in system name> to your situational understanding?	____	____	____	____	____
How important was the <fill in system name> in raising your confidence that your situational understanding was correct?	____	____	____	____	____

Quality of Individual Sensemaking: Individual Decisions	None of the time	Less than half of the time	Half of the time	More than half of the time	All of the time
How often did the <fill in system name> help you make a decision faster than you would have without using <fill in system name>?	____	____	____	____	____
	Extremely important	**Very important**	**Somewhat important**	**A little important**	**Not at all important**
How important was <fill in system name> to your decisionmaking process?	____	____	____	____	____
How important was the <fill in system name> in raising your confidence that your decision was a correct one?	____	____	____	____	____
Degree of Shared Situational Understanding Team is defined as all the people and units involved in accomplishing a task.	**None of the time**	**Less than half of the time**	**Half of the time**	**More than half of the time**	**All of the time**
How often were you confident that the entire team shared the same situational understanding?	____	____	____	____	____
How often did this system establish shared understanding within the unit?	____	____	____	____	____
with adjacent units?	____	____	____	____	____
with higher units?	____	____	____	____	____
with subordinate units?	____	____	____	____	____
with coalition units?	____	____	____	____	____
with host nation military/police units?	____	____	____	____	____

[1] Here sensemaking is defined as the process of going from awareness to understanding to decision making. See Evidence Based Research, Inc. (2004).

APPENDIX C

Statistical Analysis of Officer Impressions of Network Functionality

In this survey, officers were asked to rate network performance on a scale from 1 (excellent) to 5 (poor).

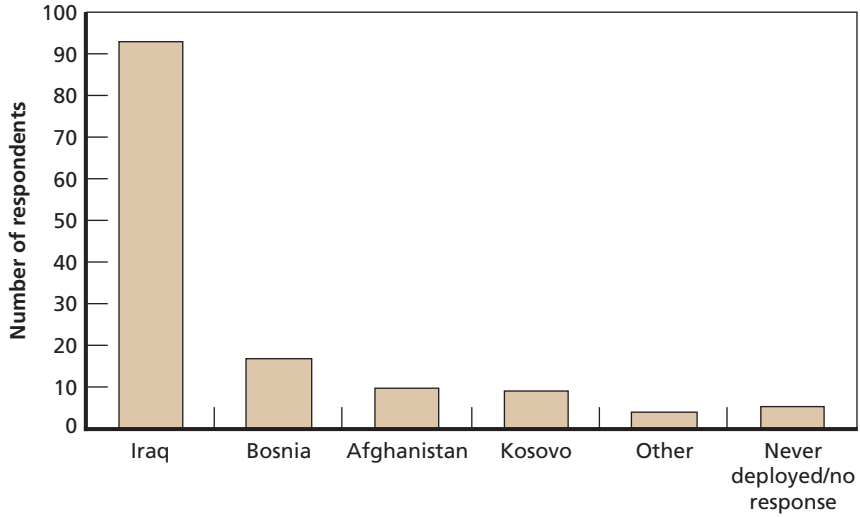
Table C.1 summarizes the characteristics of our respondents and Figure C.1 summarizes their regions of service. The figures and tables in the remainder of this appendix evaluate the network performance metrics.

Although no major differences in reach across the ranks were found, it is noteworthy that the higher-ranking officers, O-5 and O-6, generally were able to reach other units more reliably than were the lower-ranking officers. The one exception to this trend was reach to coalition units, which first lieutenants reached most reliably. The

Table C.1
Survey Respondent's Military Occupational Specialty

Rank	Infantry	Field Artillery	Other	Total
2LT	0	1	0	1
1LT	1	3	0	4
CPT	19	38	7	64
MAJ	6	7	20	33
LTC	0	5	3	8
COL	0	0	2	2
Total	26	54	32	112

Figure C.1
Distribution of Overseas Tours Among Respondents



RAND *MG788-C.1*

officers who experienced the least reliable reach were captains. Across the branches, we also found no major differences in reach capabilities. However, in the majority of cases, Signal experienced the most reliable reach to other units, and combat branches (Armor, Field Artillery, and Infantry) reported having the least reliable reach.

The functionalities of the network and network devices are not sufficient to deliver see first capabilities to the officers. The officers reported that when their primary mode of communication was not available, alternative means were available to them "most of the time" (flexibility = 3.7). However, the network speed slowed down their work about "half of the time." The network quickly adapted to changing operational needs only about "half of the time." Ironically, we received a few emails from officers in theater indicating that the network was too slow for them to fill out the survey in a reasonable amount of time. Although no major differences in network quality was found across the ranks and branches, O-6 appeared to enjoy better network flexibility,

Table C.2
Mean Network Evaluations

	Overall Network Rating	
Network	**Mean Rating**	**95 Percent Confidence Interval**
Command	2.62	(2.48, 2.77)
Sustainment	3.03	(2.81, 3.25)
Fire support	2.68	(2.47, 2.90)
Intelligence	2.83	(2.57, 3.10)
Informal	2.51	(2.31, 2.71)

NOTE: 1 = excellent, 5 = poor.

Table C.3
Summary of Network Performance Metrics

	Average Rating, by Metric	
Performance Metric	**Mean Rating**	**95 Percent Confidence Interval**
Reliability	2.27	(2.15, 2.39)
Connectivity	2.54	(2.34, 2.73)
Content	2.35	(2.22, 2.48)
Functionality	2.54	(2.41, 2.66)

NOTE: 1 = all of the time, 5 = none of the time.

speed, and adaptability than O-3. Also similar to reach capabilities, Signal responded most favorably to the network qualities.

Lieutenants and captains expressed their view that the capabilities of the network device (durability, user-friendliness, battery life, and so on) slowed down their work "half of the time." Their responses were significantly different from the responses of colonels, who reported that their work was impaired "less than half of the time." However, once again, O-6 and Signal expressed slightly favorable responses. With the

Table C.4
Response Rates, by Rank

	Eligible Respondents	
Rank	No. of Officers	Percentage
O-2: 1LT	98	9
O-3: CPT	300	29
O-4: MAJ	252	24
O-5: LTC	240	23
O-6: COL	146	14
Total	1,036	100

NOTE: Percentages do not sum to 100 because of rounding.

exception of Signal, all other branches reported that their work was affected half of the time.

"Most of the time," the officers had a radio, phone, or computer with the security level they needed. About "half of the time," operations were affected by the limited number of radios, phones, and computers. Again, there were significant differences between colonels and captains, with the limited number of devices affecting colonels less than captains. Signal also was least affected by the availability of devices.

The data on the quality of network and network devices illustrate that O-6 and Signal generally have the best reach and capabilities and that O-3 and combat branches have the worst reach and capabilities. Correlation analyses of reach (voice and text) and network and device qualities and availabilities found only weak correlations or no associations. Weak correlations were found between officers' ability to reach other units (U.S. units, coalition forces, or contractors/NGOs) and the following network and device qualities: (1) having alternative means of communication available when the primary communication mode was not available (flexibility), (2) network adapting quickly to changing operational needs (adaptability), and (3) having phones and computers with the type of security needed.

Table C.5
Response Rates, by Branch

	Eligible Respondents	
Branch	**No. of Officers**	**Percentage**
AR	164	16
FA	162	16
INF	147	14
MP	99	10
ORD	127	12
QM	98	9
SIG	154	15
TRN	85	8
Total	1,036	100

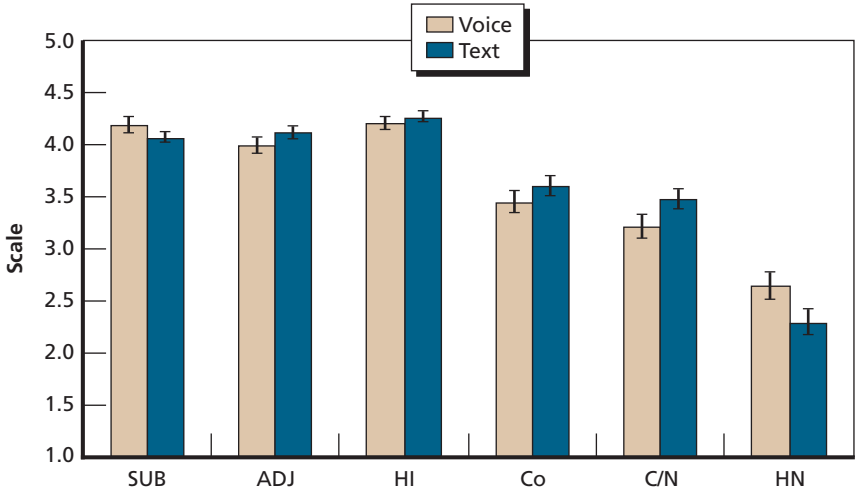
Table C.6
Officer Deployment Distribution to Iraq and Afghanistan

Deployed to	Time	No. of Officers
Iraq	Before November 2004	208
	After November 2004	668
Afghanistan	Before January 2006	64
	After January 2006	96
Total		1,036

Table C.7
Qualitative Descriptions of the Quantitative 1-to-5 Scale

Quantitative Scale	Qualitative Descriptions			
1	None of the time	None of the time	Not at all	Not at all important
2	Less than half of the time	Less than half of the time	A little bit	A little important
3	Half of the time	Half of the time	Somewhat	Somewhat important
4	More than half of the time	More than half of the time	Quite a bit	Very important
5	All of the time	All of the time	Extremely	Extremely important

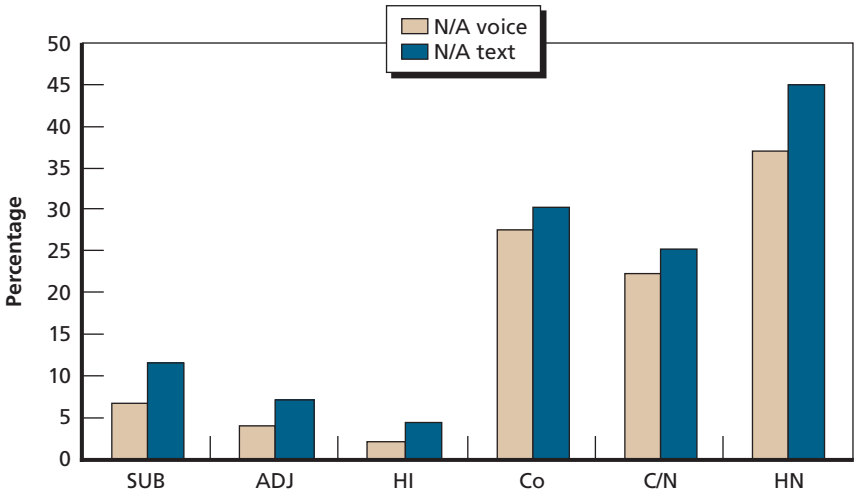
Figure C.2
How Reliably Could You Reach Other Units Using Voice or Text?



NOTE: 1 = none of the time, 5 = all of the time.

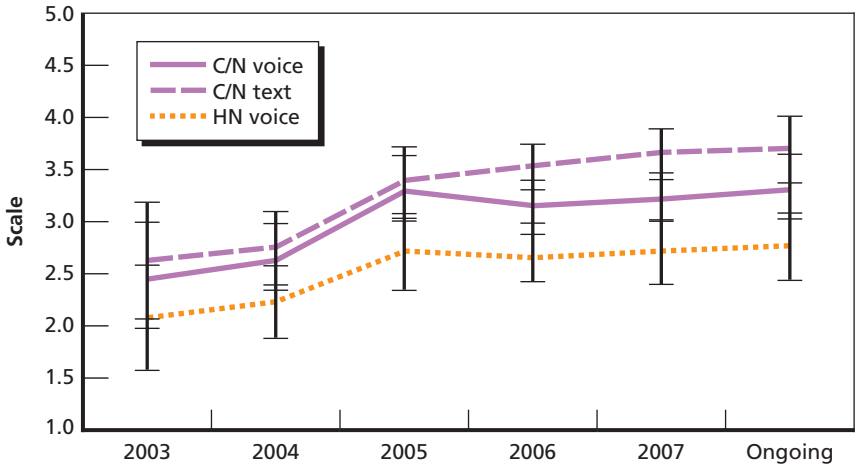
RAND *MG788-C.2*

Figure C.3
Percentage of Respondents Who Marked N/A



RAND *MG788-C.3*

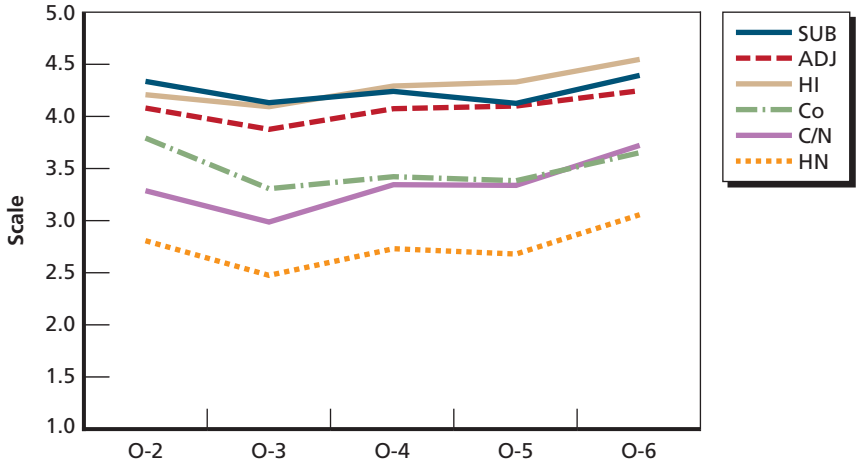
Figure C.4
Reach Reliability with Contractors/NGOs and Host Nations Improved



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.4*

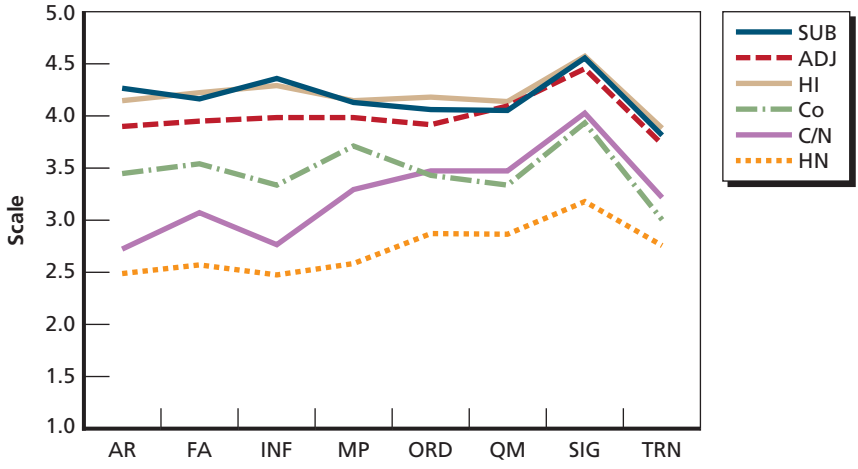
Figure C.5
Voice Reach, by Rank



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.5*

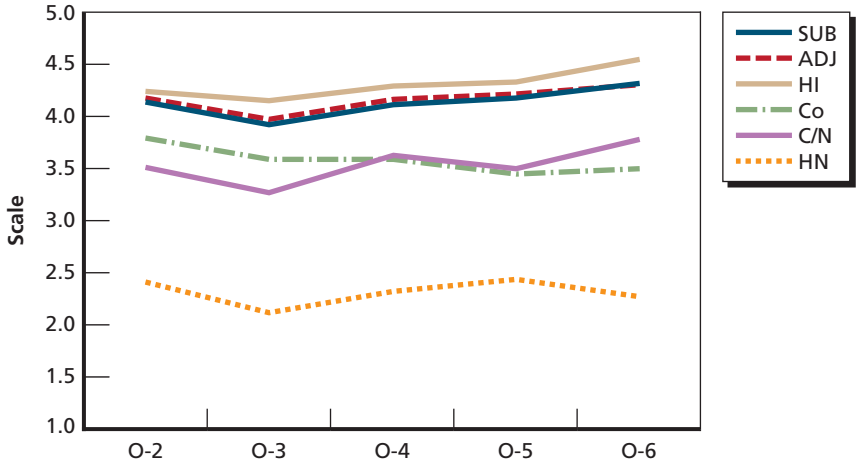
Figure C.6
Voice Reach, by Branch



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.6*

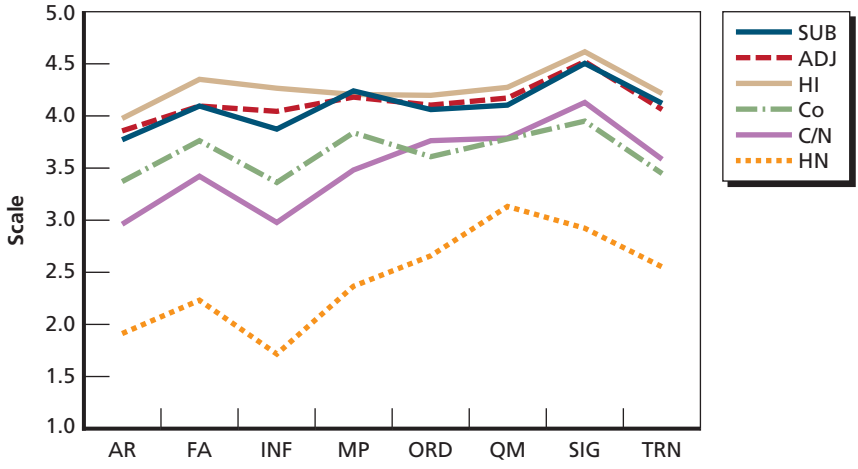
Figure C.7
Text Reach, by Rank



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.7*

Figure C.8
Text Reach, by Branch



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.8*

Table C.8
Ranks and Branches with Highest Ratings for Reach by Voice and Text

	Rank		Branch	
	Highest Rating	Significant Difference	Highest Rating	Significant Difference
Reach by Voice				
SUB	O-6	None	SIG	SIG>all except INF
ADJ	O-6	O-6>O-3	SIG	SIG>all others
HI	O-6	O-6>O-2, O-3	SIG	SIG>all others
Co	O-2[a]	O-2>O-3, O-5	SIG	SIG>AR, INF, ORD, QM, TRN
	O-6	O-6>all others	SIG	SIG>all others
HN	O-6	O-6>O-3	SIG	SIG>AR, FA, INF, ORD, MP
Reach by Text				
SUB	O-6	O-6>O-3	SIG	SIG>all except MP
ADJ	O-6	O-6>O-3	SIG	SIG>all others
HI	O-6	O-6>O-2, O-3, O-4	SIG	SIG>all except FA
Co	O-2[b]	None	SIG	SIG>AR, INF
	O-6	O-6>O-3	SIG	SIG>AR, FA, INF, MP
HN	O-5[b]	None	QM[c]	QM>AR, FA, INF

[a] O-6 gave the second-highest rating.

[b] O-6 gave the fourth-highest rating.

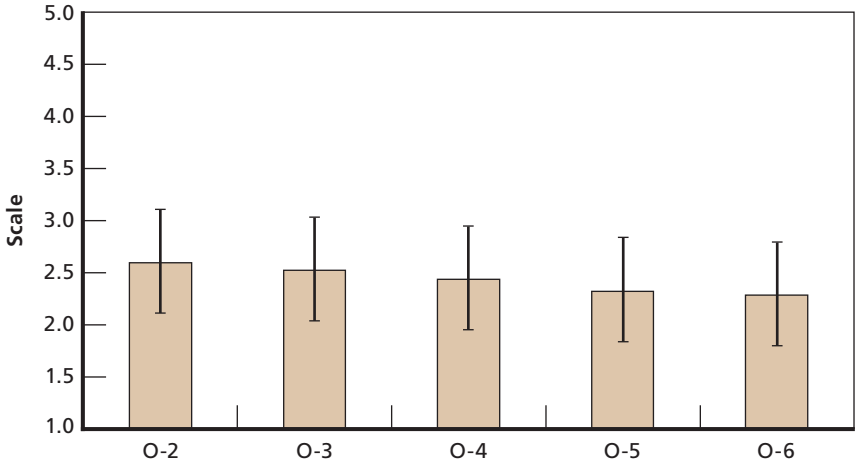
[c] Signal gave the second-highest rating.

Table C.9
Network Flexibility, Capacity, and Responsiveness, by Rank and Branch

		Rank			Branch		
Attribute	Avg.	Range	Highest Rating	Significant Difference	Range	Highest Rating	Significant Difference
Flexibility	3.7	3.52–3.99	O-6	O-6>O-3	3.28–4.28	SIG	SIG>all others
Net speed	3.26	3.22–3.57	O-6	6>O-3, O-4	2.92–3.46	SIG	SIG>ORD
Adaptability	2.96	2.87–3.27	O-6	O-6>O-3	2.61–3.31	SIG	SIG>FA, ORD

NOTE: The scale has been reversed for easier comparisons: 1 = all of the time, 5 = none of the time.

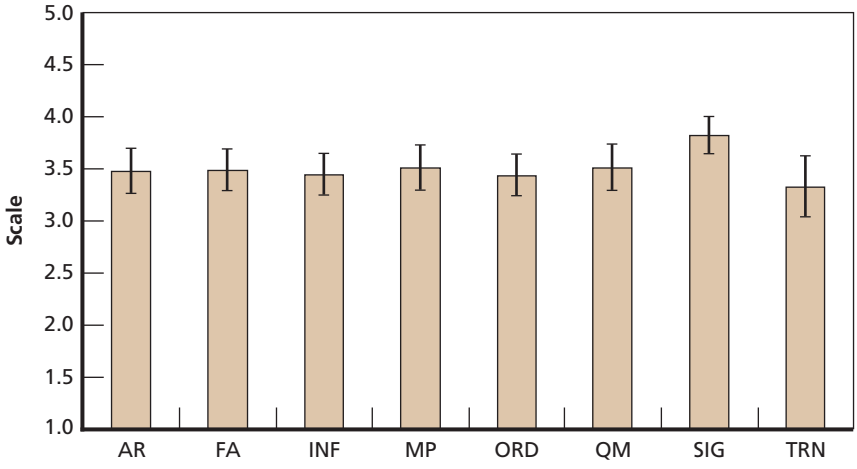
Figure C.9
Did the Capabilities of the Network Devices Slow Down Your Work? (by Rank)



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.9*

Figure C.10
Did the Capabilities of the Network Devices Slow Down Your Work? (by Branch)



RAND *MG788-C.10*

Table C.10
Was Your Operation Affected by the Limited Number of Radios, Phones, and Computers?

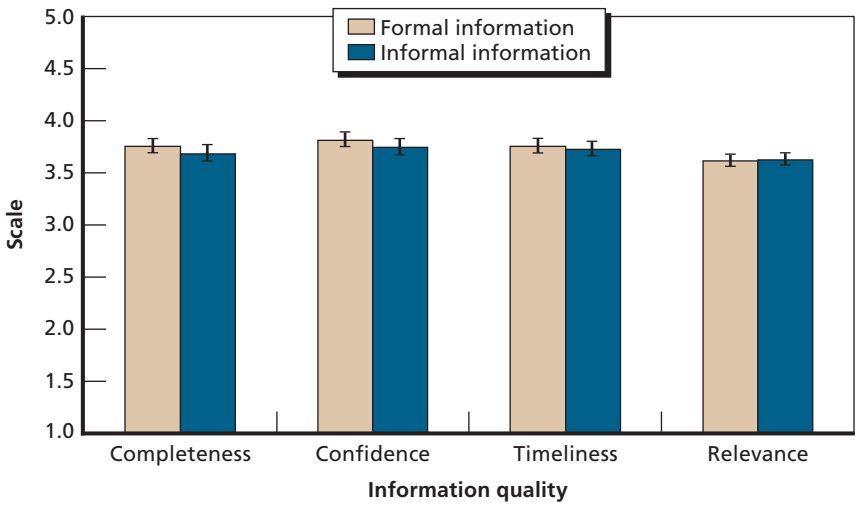
		Rank			Branch		
Device	Avg.	Range	Highest Rating	Significant Difference	Range	Highest Rating	Significant Difference
Radio	3.42	3.33–3.66	O-2	None	2.90–3.61	SIG	SIG>TRN
Phone	3.48	3.34–3.98	O-6	O-6>O-3, O-4, O-5	3.23–3.95	SIG	SIG>all except FA
Computer	3.52	3.32–4.04	O-6	O-6>O-3, O-4	3.18–3.83	SIG	SIG>QM, TRN

NOTE: The scale has been reversed for easier comparisons: 1 = all of the time, 5 = none of the time.

Table C.11
Correlations Between Device Quality and Reach

Reach Mode	Device Quality	Unit Reached					
		ADJ	HI	SUB	Co	C/N	HN
Voice	Flexibility	0.4	0.43	0.45	0.33	0.4	No assoc.
	Adaptability	0.31	0.3	0.32	0.36	0.4	No assoc.
	Phone security	0.41	0.37	0.37	0.37	0.41	0.31
	Computer security	0.39	0.41	0.38	0.36	0.38	No assoc.
Text	Flexibility	0.39	0.38	0.38	0.34	0.36	No assoc.
	Adaptability	0.37	0.32	0.36	0.36	0.35	No assoc.
	Phone security	0.47	0.45	0.42	0.44	0.42	No assoc.
	Computer security	0.55	0.56	0.53	0.45	0.45	No assoc.

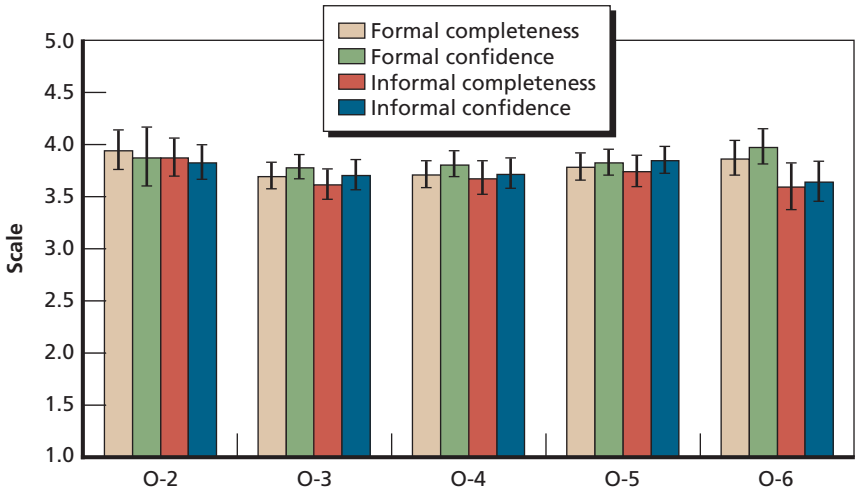
Figure C.11
Quality Comparisons of Formal and Informal Information



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.11*

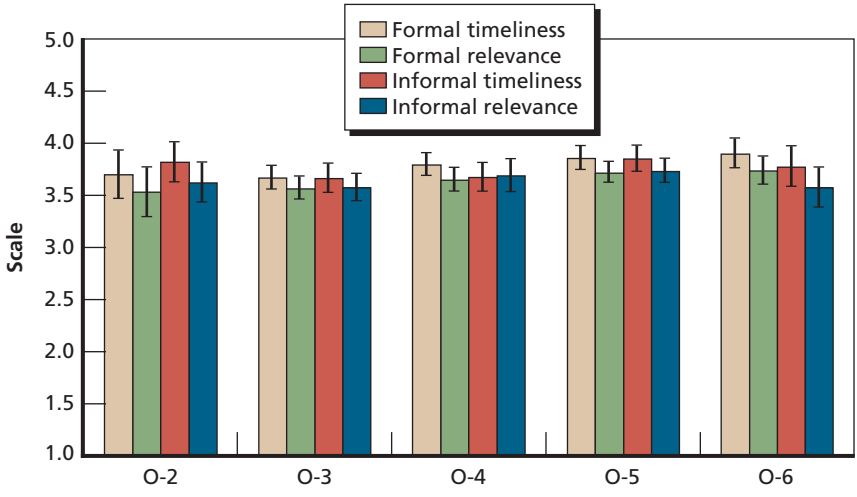
Figure C.12
Completeness of and Confidence in Information, by Rank



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.12*

Figure C.13
Timeliness and Relevance of Information, by Rank



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.13*

Table C.12
Signal Gave Highest Ratings to Information Quality

Information Quality	Formal Avg.	Significant Difference	Informal Avg.	Significant Difference
Completeness	3.75	SIG>INF, AR, TRN, ORD, QM, FA	3.68	SIG>INF, AR, ORD
Confidence	3.81	None	3.74	SIG>INF, AR, MP, TRN, ORD
Timeliness	3.75	MP>INF, AR	3.72	SIG>INF, ORD
Relevance	3.61	SIG>INF, AR	3.62	SIG>INF, AR

Table C.13
Reasons for Using Informal Network

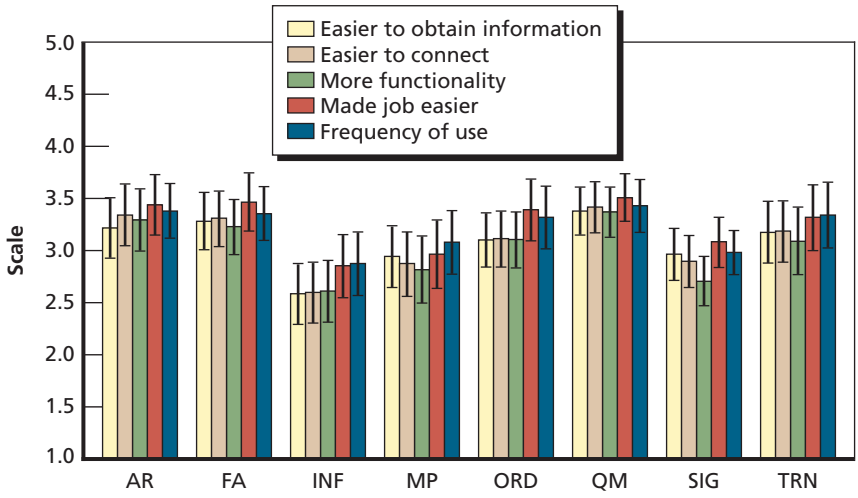
Reason	Avg.	Significant Difference
Easier to obtain information	3.04	QM>INF
Easier to connect	3.05	QM>INF, SIG
More functionalities	2.99	O5>O6; QM>INF, MP, SIG
Made job easier	3.23	QM>INF
Frequency of use	3.18	O2>O6; QM>INF

Table C.14
How Often Did You Understand All of the Information That You Needed to Accomplish Your Task? (by Rank)

	95% Confidence Interval			
Rank	Formal Information		Informal Information	
O-2	3.98	(3.78, 4.18)	3.92	(3.73, 4.11)
O-3	3.99	(3.88, 4.09)	3.85	(3.71, 3.98)
O-4	3.88	(3.78, 3.98)	3.78	(3.64, 3.93)
O-5	3.99	(3.87, 4.10)	3.93	(3.80, 4.07)
O-6	4.00	(3.85, 4.15)	3.85	(3.66, 4.04)

NOTE: 1 = none of the time, 5 = all of the time.

Figure C.14
Reasons for Using Informal Network, by Branch



NOTE: 1 = none of the time, 5 = all of the time.

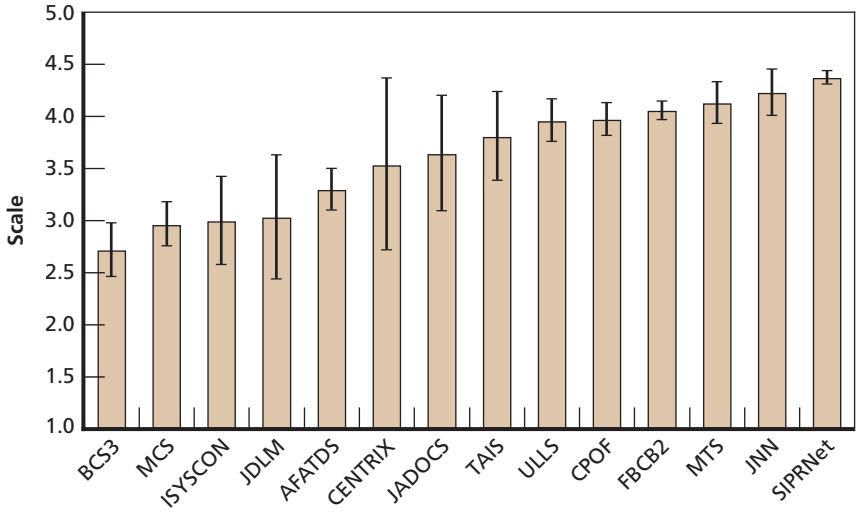
RAND *MG788-C.14*

Table C.15
How Often Did You Understand All of the Information That You Needed to Accomplish Your Task? (by Branch)

	95% Confidence Interval			
Branch	**Formal Information**		**Informal Information**	
AR	3.95	(3.81, 4.09)	3.87	(3.73, 4.01)
FA	4.09	(3.95, 4.22)	3.99	(3.81, 4.18)
INF	3.89	(3.71, 4.06)	3.71	(3.48, 3.93)
MP	4.13	(3.99, 4.28)	3.77	(3.55, 4.00)
ORD	3.88	(3.71, 4.04)	3.73	(3.54, 3.92)
QM	3.86	(3.69, 4.04)	3.83	(3.63, 4.03)
SIG	4.02	(3.87, 4.17)	4.06	(3.93, 4.19)
TRN	3.86	(3.68, 4.04)	3.83	(3.57, 4.09)

NOTE: 1 = none of the time, 5 = all of the time.

Figure C.15
How Important Was the System to Your Situational Understanding?



NOTE: 1 = not at all important, 5 = extremely important.
RAND *MG788-C.15*

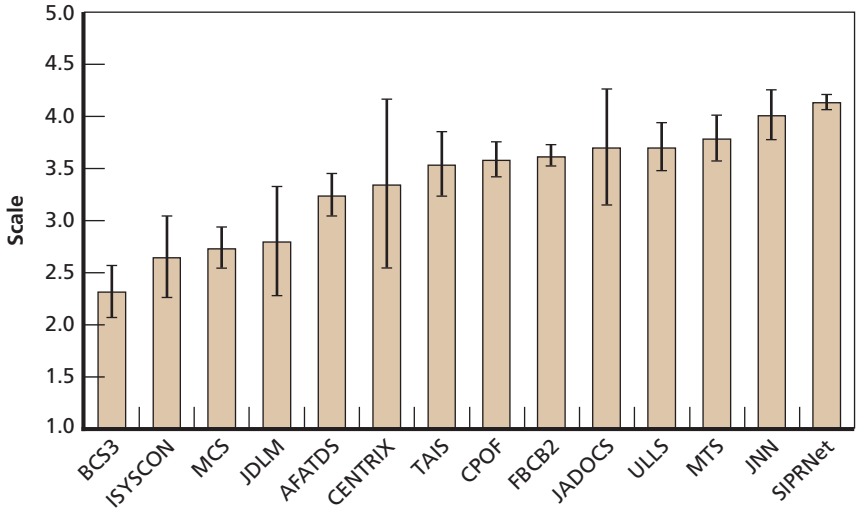
Table C.16
Formal System Function in Officer Situational Understanding

	95% Confidence Interval		
	SIPRNet	**FBCB2**	**CPOF**
Understand more completely[a]	4.19 (4.11, 4.25)	3.8 (3.71, 3.89)	3.87 (3.73, 4.02)
Understand faster[a]	4.19 (4.11, 4.27)	3.83 (3.73, 3.92)	3.89 (3.74, 4.04)
Raised confidence in situational understanding[a]	4.28 (4.22, 4.35)	3.99 (3.90, 4.08)	3.85 (3.69, 4.01)
Importance to situational understanding[b]	4.36 (4.29, 4.43)	4.05 (3.96, 4.14)	3.96 (3.81, 4.12)

[a] 1 = none of the time, 5 = all of the time.

[b] 1 = not at all important, 5 = extremely important.

Figure C.16
How Important Was the System to Your Decisionmaking Process?

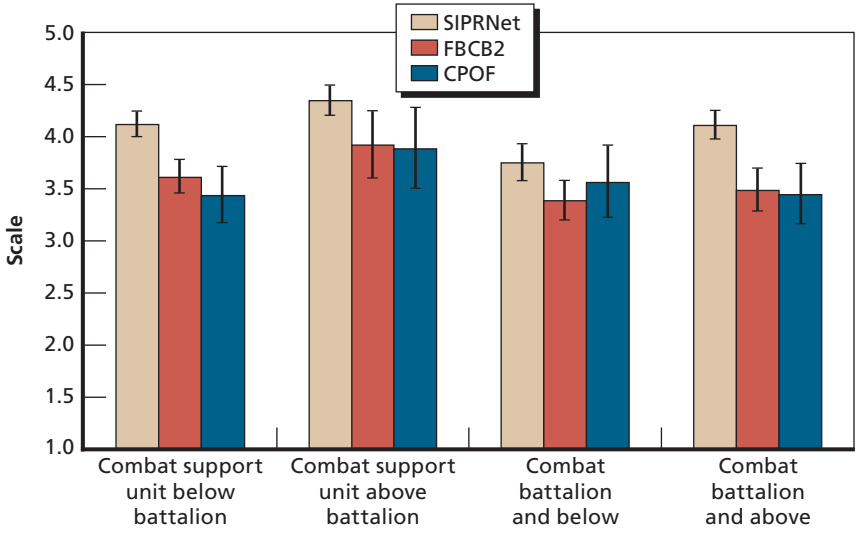


NOTE: 1 = not at all important, 5 = extremely important.
RAND *MG788-C.16*

Table C.17
Correlations Between Cognitive Domain Attributes and System User-Friendliness

Cognitive Domain Attribute	SIPRNet	FBCB2	CPOF
Understand completely	0.45	0.48	0.62
Understand faster	0.45	0.44	0.62
Faster decisionmaking	0.43	0.41	0.6

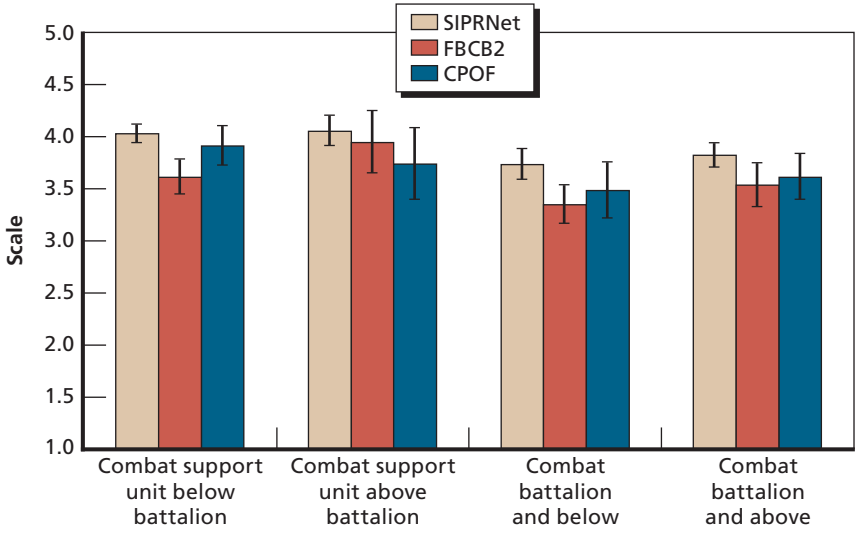
Figure C.17
How Often Did This System Help You Make Your Decision Faster Than You Would Have Without the System?



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.17*

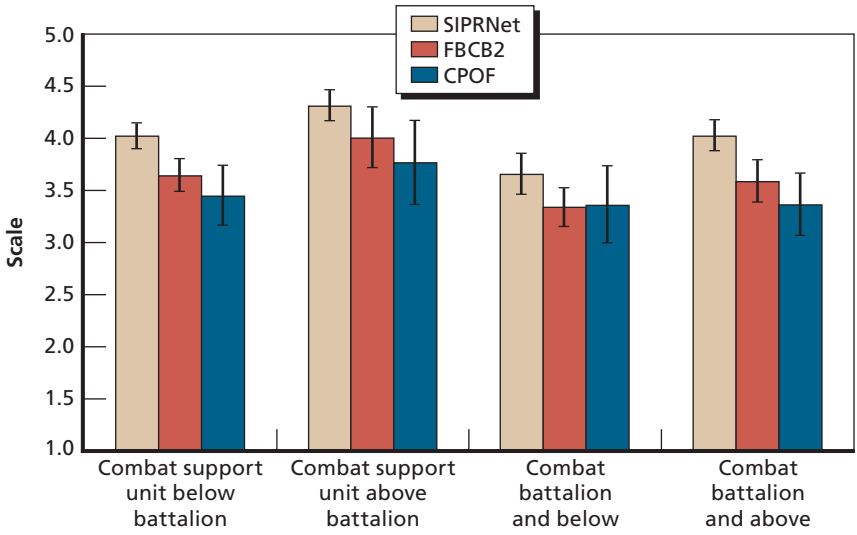
Figure C.18
How Important Was the System in Raising Your Confidence That Your Decision Was a Correct One?



NOTE: 1 = not at all important, 5 = extremely important.

RAND *MG788-C.18*

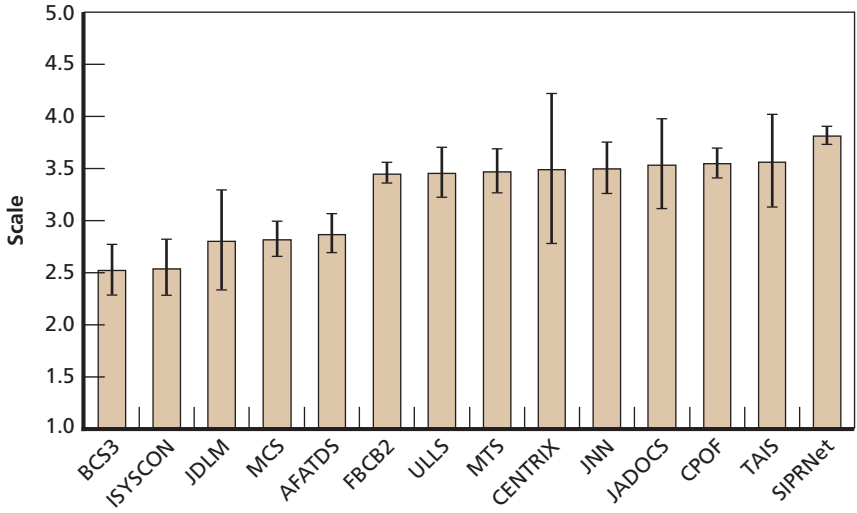
Figure C.19
How Important Was the System to Your Decisionmaking Process?



NOTE: 1 = not at all important, 5 = extremely important.

RAND *MG788-C.19*

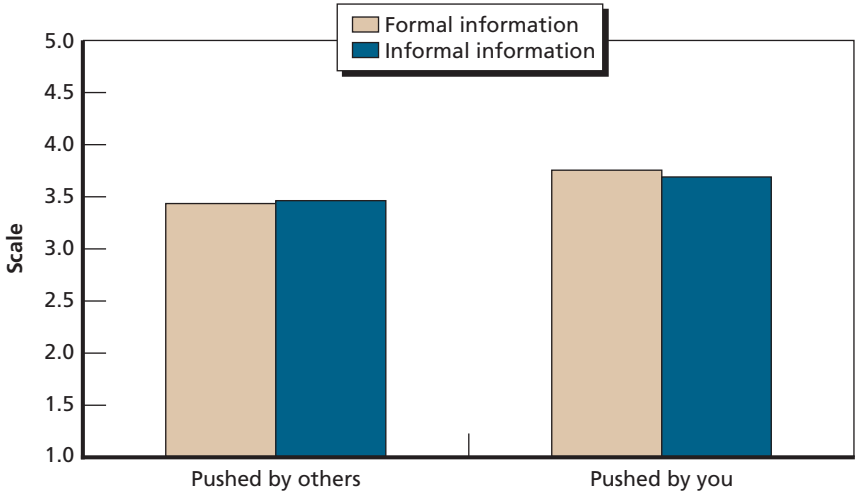
Figure C.20
To What Degree Was the System User-Friendly?



NOTE: 1 = not at all, 5 = extremely.

RAND *MG788-C.20*

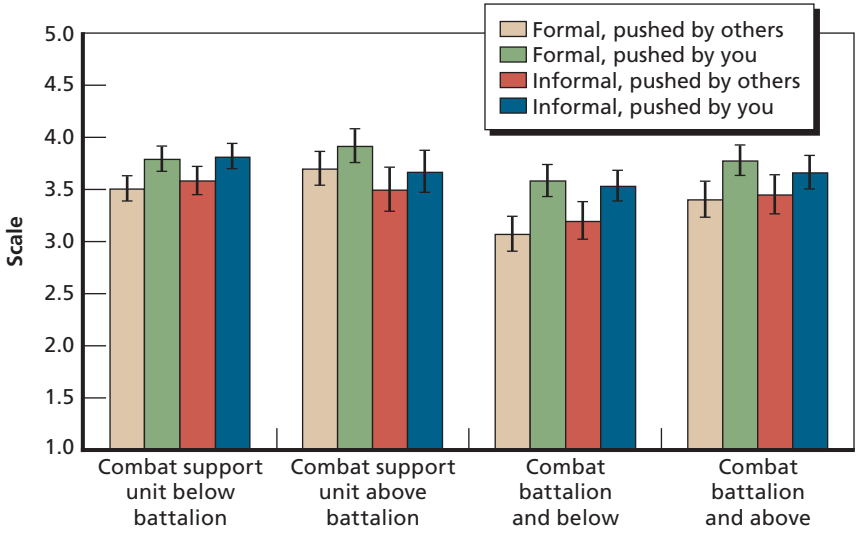
Figure C.21
How Often Did Other Units Push Information to You or How Often Did You Push Information to Others?



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.21*

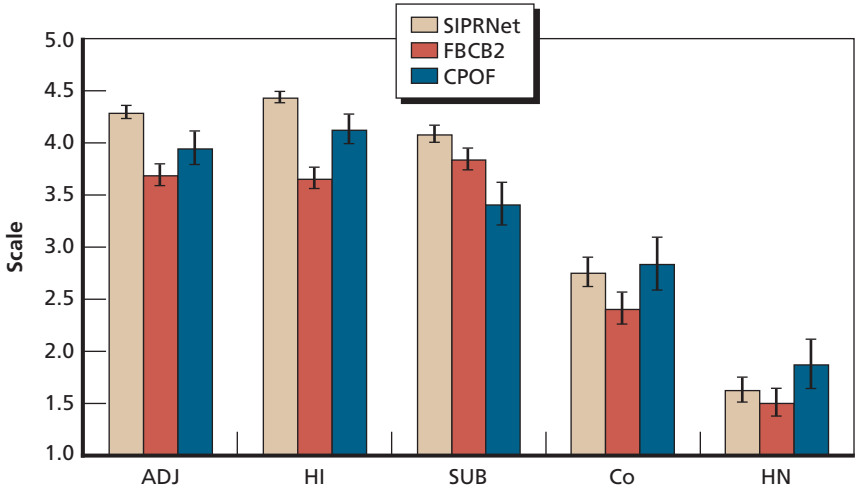
Figure C.22
How Often Did Other Units Push Information to You or How Often Did You Push Information to Others?



NOTE: 1 = none of the time, 5 = all of the time.

RAND *MG788-C.22*

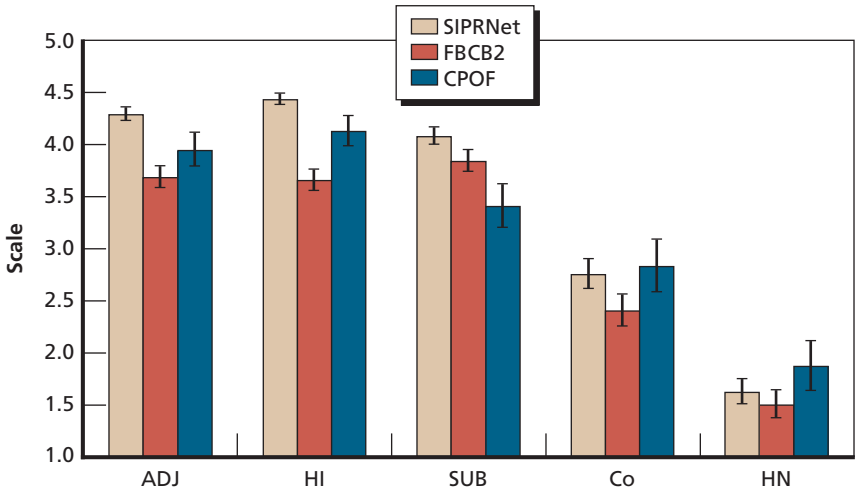
Figure C.23
How Reliably Did the System Facilitate Sharing of Information with Other Units?



NOTE: 1 = not at all, 5 = extremely.

RAND *MG788-C.23*

Figure C.24
How Often Did This System Establish Shared Understanding?



NOTE: 1 = not at all, 5 = extremely.

RAND *MG788-C.24*

APPENDIX D

Statistical Analysis of Unit Performance Data from the National Training Center

Using Data from the National Training Center

One source of insight on the utility of digital C2 systems is exercises at the National Training Center. As part of RAND's work at the NTC, observers/controllers fill out special RAND forms for platoon, company, and battalion missions that assess the unit's performance on a variety of dimensions using a six-point scale ("not done" to "superior"). The dimensions include planning, situational awareness, force protection, interaction with subordinate and higher levels, and an overall assessment of unit performance. Of interest for our purposes are the questions on the use of digital command, control, communication, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems that indicate how well the unit used these systems (see Table D.1).

The specific data we used were collected during NTC rotations from March 2005 through March 2006. National Guard units were eliminated because most if not all did not have the digital C2 systems of interest. Each active-duty NTC rotation is structured around a battalion, which is given several missions. In carrying out those missions, companies and platoons are assigned specific missions and tasks, such as reconnaissance, movement to contact, and hasty attack. During these particular rotations, substantial time is spent on counterinsurgency tasks, for example, dealing with IEDs and civilian populations. Each task and mission was rated by the observers/controllers

Table D.1
Questions on the Use of Digital C4ISR Systems for Each Level of Unit

Battalion
Complete following forms ONLY for Army Battle Command Systems (ABCS). How well did the battalion . . .
Set up, operate, and maintain FBCB2/BFT?
Set up, operate, and maintain MCS?
Set up, operate, and maintain ASAS?
Set up, operate, and maintain AFATDS?
Set up, operate, and maintain CSCSS?
Post digital graphics?
Use ABCS systems to keep higher informed?
Conduct digital rehearsals?
Use digital systems to C2 their elements?
Appropriately use ABCS (e.g., not when should have been using other means)?
Maintain back up/work around systems as necessary?
Company
Complete the following items ONLY in terms of DIGITAL C4ISR Systems (e.g., FBCB2 or BFT). How well did the unit . . .
Set up, operate, and maintain digital systems?
Use to C2 the company?
Use to keep higher informed?
Appropriately use (e.g., not used when should have used other means)?
Platoon
Complete the following items ONLY in terms of DIGITAL C4ISR Systems (e.g., FBCB2 or BFT). How well did the platoon . . .
Set up, operate, and maintain digital systems?
Use digital systems?

on the RAND forms, but, given the type of mission, some items may have been omitted.

Although the information on digital system use is most detailed at the battalion level, we have only 21 records for battalion missions, and these constitute only nine battalions. These very limited data are not suitable for statistical analysis and so were not analyzed further. The data for platoons and company missions are more plentiful (284 and 94, respectively), although some of these observations involve missions carried out by the same unit. A more complete analysis would take this overlap into account.

Company Analysis

The observers/controllers rated each company's use of digital C4ISR systems in a mission by rating them on the four company questions listed in Table D.1.

For our analysis, we used the first three questions to rate how well the unit used the digital C4ISR systems available. A company was deemed to have used the systems well when the answers to the first three were all "moderate," "complete," or "superior," otherwise they were deemed to not have used the systems adequately ("not used," "not sufficient," "somewhat").

For combat performance we looked individually at the following questions. Throughout the operation, how well did the company

- maintain situational awareness?
- maintain situational understanding?
- issue timely orders and keep subordinates updated?
- control and synchronize subordinate organizations?
- coordinate with adjacent, supporting, and supported organizations?
- maintain internal communication?
- meet required times to execute actions?
- provide constant, all-around observation?
- detect and report all enemy and intelligence/information requirements?
- synchronize patrols to ensure that objective areas were fully covered?
- take actions to avoid fratricide?
- find, fix, and destroy the enemy?
- identify and detail appropriate individuals?
- find and react to IEDs/VBIEDs/mines/unexploded ordnance?
- operate with/with support from
  a. NGOs?
  b. local police and military?
  c. coalition forces?

d. Special Operations Forces (SOF)/the Central Intelligence Agency (CIA)?
e. other U.S. joint elements?

How well were negotiation objectives achieved? How well was route security conducted? When assigned a QRF mission, how well did the company

- respond quickly to orders to move?
- coordinate with friendly forces and avoid fratricide?
- accomplish the mission?

How well were assigned missions and tasks accomplished?

For all of these individual questions, the unit was deemed to have performed that mission/task adequately if the observer/controller rated its performance "moderate" to "superior," otherwise it was considered an inadequate performance.

To analyze the correlation between use of digital C4ISR systems and performance on these missions/tasks, we constructed a series of 2 × 2 tables (adequate/inadequate on digital C4ISR use versus adequate/inadequate performance on the individual task or mission). The digital C4ISR use versus overall performance is illustrated in Table D.2.

For this type of table, if there are high counts on the diagonal, the two variables are positively correlated (digital C4ISR use is observed with good task performance, and inadequate use of digital C4ISR is observed with poor task performance); if there are high counts on the off-diagonal, the variables are negatively correlated (digital C4ISR use is observed with poor task performance and inadequate use of digital

Table D.2
Overall Performance Versus Use of Digital C4ISR

Performance	Digital C4ISR Use Good	Digital C4ISR Use Inadequate
Good	24	3
Inadequate	29	20

C4ISR is observed with good performance). A third possibility is that the two variables are not related if the counts do not show either of these two patterns. Although many statistics have been developed to quantify the relationship, we elected to use the phi coefficient. This quantity is constrained by definition to lie between –1 and 1 (negative and positive correlation), with values close to 0 indicating no relationship.

One general rule of thumb for correlation coefficients such as phi is the following:

–1.0 to –0.7, strong negative association
–0.7 to –0.3, weak negative association
–0.3 to +0.3, little or no association
+0.3 to +0.7, weak positive association
+0.7 to +1.0, strong positive association.

Table D.3 gives the phi coefficient and its p-value for the 2 × 2 table relating use of digital C4ISR systems with good performance in each of the tasks. Note that the total number of observations in each row is not 94 because not each unit was rated on each performance measure; whether it was rated or not depended on the unit's mission.

The missions/tasks that are both significantly different from zero and that show a weak positive correlation with digital C4ISR system use are highlighted. Note that none of the missions shows a strong positive correlation according to the rule of thumb cited. However, overall performance and QRF performance does show an effect, as does operation with coalition forces and finding/reacting to explosives. None of the missions required working with SOF/CIA or NGOs.

Platoon Analysis

The analysis of platoon use of digital C4ISR systems paralleled the company analysis, although, as shown in Table D.1, the information collected on platoon digital system use was less detailed.

As with the company data, we elected to combine these two questions into a single variable indicating whether the platoon used digital systems well or not. As with the company data, we rated a platoon's use as good if the observer controller rated it "moderate" to "superior"

Table D.3
Phi Coefficient for Company Performance Rating Versus Use of Digital C4ISR Systems

Mission/Task	No.	Phi	P
Throughout . . . maintain situational awareness?	81	–0.002	0.98
Throughout . . . maintain situational understanding?	81	0.065	0.56
Throughout . . . issue timely orders and keep subordinates updated?	81	0.25	0.03
Throughout . . . control and synchronize subordinate organizations?	81	0.23	0.04
Throughout . . . coordinate with adjacent, supporting, and supported organizations?	80	0.15	0.19
Throughout . . . maintain internal communication?	81	0.2	0.07
Throughout . . . meet required times to execute actions (for example, line of defense, "no later than" times)?	80	0.43	0.0001
Throughout . . . provide constant all-around observation?	81	0.25	0.03
Throughout . . . detect and report all enemy and intelligence/information requirements?	77	0.19	0.09
Throughout . . . synchronize patrols to ensure that objective area is fully covered?	75	0.07	0.53
Throughout . . . take actions to avoid fratricide?	79	0.18	0.1
Throughout . . . find, fix, and destroy enemy?	71	–0.004	0.97
How well did the company identify and detain appropriate individuals?	54	0.18	0.2
How well did the company find and react to IEDs/VBIEDs/ mines/unexploded ordnance?	62	0.365	0.004
Operate with support from NGOs?	0	N/A	N/A
Operate with support from local police and the military?	41	0.1	0.51
Operate with support from coalition forces?	25	0.52	0.01
Operate with support from SOF/CIA?	0	N/A	N/A
Operate with support from other U.S. joint elements?	17	0.66	0.01
How well was route security conducted?	57	0.05	0.71
QRF mission . . . respond quickly to orders to move?	50	0.35	0.01
QRF mission . . . coordinate with friendly forces and avoid fratricide?	50	0.53	0.0002
QRF mission . . . accomplish mission?	50	0.49	0.0006
How well were assigned missions and tasks accomplished?	76	0.31	0.007

on both questions and as inadequate if it was rated "not done" to "somewhat" on either of the two questions.

For combat performance measures, we selected the following questions from the observer/controller forms. Throughout the operation, how well did the platoon

- maintain situational awareness?
- issue timely orders and keep subordinates updated?
- control platoon?
- coordinate with adjacent, supporting, and supported organizations?
- maintain internal communication?
- provide constant, all-around observation
- detect and report all enemy and intelligence/information requirements?
- take actions to avoid fratricide?
- use indirect fire?

When assigned a QRF mission, how well did the platoon

- respond quickly to orders to move?
- coordinate with friendly forces and avoid fratricide?
- accomplish mission?
- conduct presence patrols?
- accomplish assigned missions and tasks?

As in the company analysis, we examined the correlation between use of digital C4ISR systems and each of these measures by constructing 2 × 2 tables and computing the phi coefficient for each. The results are shown in Table D.4.

As with the company data, the entries that are statistically different from zero and have moderate positive correlations are highlighted.

First, note that the data for the platoons tend to be more sparse: In spite of having 284 records for platoons, generic evaluations, such as overall success or maintaining situational awareness, are rated only for use of digital C4ISR systems in 160 to 190 observations. Another

Table D.4
Phi Coefficient for Platoon Performance Rating Versus Use of Digital C4ISR Systems

Mission/Task	No.	Phi	p
How well were assigned missions and tasks accomplished?	163	0.154	0.05
Throughout . . . maintain situational awareness?	190	0.18	0.01
Throughout . . . issue timely orders and keep subordinates updated?	191	0.1	0.17
Throughout . . . control platoon?	192	0.23	0.002
Throughout . . . coordinate with adjacent, supporting, and supported organizations?	180	0.06	0.46
Throughout . . . maintain internal communication?	190	0.42	<0.0001
Throughout . . . provide constant all-around observation?	190	0.17	0.02
Throughout . . . detect and report all enemy and intelligence/information requirements?	173	0.26	0.0006
Throughout . . . take actions to avoid fratricide?	180	0.46	<0.0001
Throughout . . . use indirect fire?	39	0.21	0.2
QRF mission . . . respond quickly to orders to move?	86	0.25	0.021
QRF mission . . . coordinate with friendly forces and avoid fratricide?	86	0.37	0.0006
QRF mission . . . accomplish mission?	85	0.37	0.0006
How well did platoon conduct presence patrols?	82	0.21	0.06

striking point is that overall mission/task success is just barely significantly correlated with digital system use, and the correlation is quite small. However, avoiding fratricide and performance on two of four QRF dimensions is positively weakly correlated with digital system use, as is maintenance of internal communication.

Results

A number of qualifications should be kept in mind about this analysis. First, some of the observations for both companies and platoons are for the same units doing different missions. In addition, some observers/

controllers are the same across different rotations. For these reasons, the observations are not strictly independent. Further, the data include all missions/tasks by non–National Guard units at the NTC, so the individual missions/tasks are not necessarily homogeneous, nor are all the units of the same type (this is especially true for platoons). However, these results do provide a first look at the relation between digital C4ISR use and some selected performance measures.

The effects at company level are stronger; in particular, overall mission accomplishment is positively correlated with digital C4ISR system use. We speculate that this is because companies are large enough to "pay the overhead" to operate such systems. However, it is worth noting that both companies and platoons perform well on QRF missions, which is also positively correlated with digital system use.

Selected Bibliography

1/1 TST Operations and Targeting, briefing, December 27, 2007.

Agron, COL Gary, and Col Charles Pattillo, "Network Centric Operations: The Power of Information Age Concepts and Technologies," Office of Force Transformation, Office of the Secretary of Defense.

Akam, LTC Bob, Division G3, 1st Cavalry Division, "Task Force Baghdad: Operation Iraq Freedom II," briefing, undated.

Alberts, D. S., J. J. Garstka, and F. P. Stein, *Network-Centric Warfare: Developing and Leveraging Information Superiority,* 2nd ed., Washington, D.C.: C4ISR Cooperative Research Program, 1999.

Allawi, Ali A., *The Occupation of Iraq: Winning the War and Losing the Peace,* London, U.K., and New Haven, Conn.: Yale University Press, 2007.

American Forces Press Service, "Unmanned Predator Kills Three Terrorists; Relative Turns in Suspect," March 29, 2006. As of July 2008: http://www.defenselink.mil/news/Mar2006/20060329_4648.html

Antonietti, LTC Patrick M., and CPT Donald K. Brooks, "A Fires Battalion in OIF III: Supporting Decentralized 'Hot' Platoons and Other Missions," *Field Artillery,* July–August 2006, pp. 28–32.

Army Public Affairs, "'Ironhorse' Division Assumes Responsibility for Baghdad," Army News Service (ARNEWS), January 9, 2006. As of February 5, 2009: http://www.globalsecurity.org/military/library/news/2006/01/mil-060109-arnews03.htm

Arnas, Neyla, Charles Barry, and Robert B. Oakley, *Harnessing the Interagency for Complex Operations,* Washington, D.C.: National Defense University, Center for Technology and National Security Policy, August 2005. As of July 2008: http://www.ndu.edu/ctnsp/def_tech/dtp%2016%20harnessing%20the%20interagency.pdf

Asymmetric Warfare Group, "Command Staff Update—1-1 BCT Intro to F3EAD Methodology," briefing, December 20, 2006.

Baker, COL Ralph O., U.S. Army, "The Decisive Weapon: A Brigade Combat Team (BCT) Commander's Perspective on Information Operations (IO)," briefing presented at the Information Operations Symposium II, Ft. Leavenworth, Kan., December 15, 2005.

Batiste, MG John R.S., U.S. Army, and LTC Paul R. Daniels, U.S. Army, "The Fight for Samarra: Full-Spectrum Operations in Modern Warfare," *Military Review,* May–June 2005, pp. 13–21. As of July 2008: http://www.army.mil/professionalWriting/volumes/volume3/september_2005/9_05_3.html

Bell, GEN Burwell B., U.S. Army, MGEN Guy M. Bourn, U.S. Army, COL Nathan K. Slate, U.S. Army, and LTC David D. Haught, U.S. Army, "The New DOCC," *Military Review,* January–February 2003, pp. 37–41.

Bell, Gertrude L., C.B.E., *Review of the Civil Administration of Mesopotamia,* London, U.K.: His Majesty's Stationery Office, 1920.

Bell, SGT Mark, "Troops Transfer Authority of Baghdad's Al Rashid District," Defend America—U.S. Department of Defense News About the War on Terrorism, January 29, 2004.

Belote, COL Dave, Ft. Hood, Tex.: 3rd ASOG, unpublished.

Bird, RADM John M., U.S. Navy, J3/4, Director, Operations & Logistics, J3/4, "Global Force Management Board," U.S. Joint Forces Command, unpublished briefing, May 11, 2005.

Blair, ADM Dennis C., U.S. Navy, "We Can Fix Acquisition," *Proceedings,* May 2002. As of July 2008: http://www.usni.org/magazines/proceedings/archive/month.asp?ID=119

Boddy-Evans, Alistair, "Timeline: Mau Mau Rebellion: April 1954 to Present Day," undated. As of June 2008: http://africanhistory.about.com/od/kenya/a/MauMauTimeline_2.htm

Boutelle, LTG Steven W., "LandWarNet Is New Name for Army Network," U.S. Army News Release, Army Public Affairs, Washington D.C., February 26, 2004.

Bowman, Steve, Lawrence Kapp, and Amy Belasco, *Hurricane Katrina: DoD Disaster Response,* CRS Report for Congress, Washington, D.C.: Congressional Research Service, Library of Congress, Order Code RL33095, October 6, 2005.

Bowman, Tom, "A 'Lessons Learned' Review," *Baltimore Sun,* February 23, 2006, p. 2A.

Boyle, LTC Brian T., and LTC William M. Raymond, Jr., "NLOS Battalion: Fires and Effects in the UA of 2015," *Field Artillery,* May–June 2003, pp. 32–38.

Braganca, Maj Eric P., U.S. Air Force, "Joint Fires Evolution," *Military Review,* January–February 2004, pp. 50–53.

Britain's Small Wars, "The RAF in Kenya," 2008. As of June 2008: http://www.britains-smallwars.com/kenya/RAF.html

Bronson, John L., Chief Information Office, U.S. Army, "Army LandWarNet Evolution," presentation to the Army Science Board, March 15, 2007.

Brown, GEN Bryan D., U.S. Army, Commander, U.S. Special Operations Command, Testimony Before the United States House of Representatives, Committee on Armed Services, Subcommittee on Terrorism, Unconventional Threats and Capabilities, regarding the Special Operations Command Budget Request for Fiscal Year 2005, March 11, 2004.

Brown, Col David R., U.S. Air Force, "JTAC MOA vs. JTTP," *Field Artillery,* January–February 2005, pp. 18–21.

Brown, John S., "Unit Designations in Our New Modular Army," *Army,* November 1, 2005.

Brown, LTC Robert B. "The Agile-Leader Mindset: Leveraging the Power of Modularity in Iraq," *Military Review,* July–August 2007.

Bush, George W., *The National Security Strategy of the United States of America,* September 17, 2002. As of March 3, 2009: http://www.globalsecurity.org/military/library/policy/national/nss-020920.pdf

———, *The National Strategy to Combat Weapons of Mass Destruction,* December 11, 2002. As of March 3, 2009: http://www.cfr.org/publication/9066/national_strategy_to_combat_weapons_of_mass_destruction.html

———, *The National Security Strategy of the United States of America,* March 2006. As of March 3, 2009: http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/

Cahill, LTC Dennis J., U.S. Army Headquarters (G-37FM), "Strengthening Civil Affairs Capability: An Holistic Approach," draft briefing, August 24, 2005. Not available to the general public.

Campbell, COL, "Task Force Observe, Detect, Identify and Neutralize (TF ODIN) Update," ARCIC AWD, U.S. Army Training and Doctrine Command, July 10, 2007.

Carty, MAJ William J., U.S. Army, "An Unconventional Look at Training and Education to Improve Conventional and SOF Integration," paper submitted to the National Defense Industrial Association–Special Operations and Low Intensity Conflict Division and Joint Special Operations University for competition in the 2004 Special Operations and Low Intensity Conflict Essay Contest, January 15, 2004.

Cassidy, LTC Robert M., U.S. Army, "The British Army and Counterinsurgency: The Salience of Military Culture," *Military Review,* May–June 2005, pp. 53–59.

Center for Army Lessons Learned, *82nd Airborne Division Initial Impressions Report—Observations and Lessons Learned,* Task Force Devil, OEF, December 2002–September 2003, Ft. Bragg, N.C., January 2004.

———, *Operation Iraqi Freedom (OIF) CAAT II Initial Impressions Report,* CALL Newsletter 04-13, May 2004. As of July 2008: http://www.globalsecurity.org/military/library/report/call/call_04-13_toc.htm

———, "Cordon and Search: Tactics, Techniques, and Procedures," CALL Handbook No. 04-16, Ft. Leavenworth, Kan., July 2004.

———,"Initial Impressions Report, Operations in Mosul, Iraq—Stryker Brigade Combat Team 1," 3rd Brigade, 2nd Infantry, Ft. Leavenworth, Kan., December 21, 2004. Not available to the general public.

———, "Special Operations Forces/Conventional Forces Integration," Initial Impressions Report No. 05-33, Ft. Leavenworth, Kan., August 2005.

———, *Disaster Response/Hurricanes Katrina and Rita,* Initial Impressions Report, No. 06-11, Ft. Leavenworth, Kan., February 2006.

Center for Military History Online, "The United States Army in Afghanistan: Operation Enduring Freedom," October 2001–March 2002. As of July 2008: http://www.history.army.mil/brochures/Afghanistan/Operation%20Enduring%20Freedom.htm

Chase, LTC "Chip," U.S. Joint Chiefs of Staff, "Joint Staff Perspective on Combating WMD," unpublished briefing, May 16, 2006.

Chelberg, LTG (Ret.) Robert D., COL Jack W. Ellertson, and MAJ David H. Shelley, "EUCOM: At the Center of the Vortex," *Field Artillery,* October 1993, pp. 12–16.

Chiarelli, MG Peter W., U.S. Army, "Task Force Baghdad, Operation Iraqi Freedom II," briefing to the Command and General Staff Officer Course, April 1, 2005.

Chiarelli, MG Peter W., U.S. Army, MAJ Patrick R. Michaelis, U.S. Army, and MAJ Geoffrey A. Norman, U.S. Army, "Armor in Urban Terrain: The Critical Enabler," *Armor,* March–April 2005, pp. 7–12.

Chiarelli, MG Peter W., U.S. Army, and MAJ Patrick R. Michaelis, U.S. Army, "Winning the Peace: The Requirement for Full-Spectrum Operations," *Military Review*, July–August 2006, pp. 4–17.

Chiarelli, MG Peter W., U.S. Army, and MAJ Stephen M. Smith, U.S. Army, "Learning from Our Modern Wars: The Imperatives of Preparing for a Dangerous Future," *Military Review,* September–October 2007, pp. 2–15.

"CJTF-7 OIF Force Flow Conference," Scott Air Force Base, Ill., briefing, May 3–14, 2004.

Clodfelter, Michael, *Warfare and Armed Conflicts: A Statistical Reference,* Vol. II, Jefferson, North Carolina, and London, U.K.: McFarland and Company, Inc., 1992.

Cloud, David S., "Violence Rising in Much of Iraq, Pentagon Says," *New York Times,* June 14, 2007.

Cody, GEN Richard A., Vice Chief of Staff, U.S. Army, handwritten note shared with the authors at HQDA G-3/5/7, The Pentagon, Arlington, Va., January 25, 2007.

Combatant Commander's Planning Guide for WMD Elimination Operations, Annex D, JTF-E: Organizational and Operational Considerations, pp. D-1–D-9. Not available to the general public.

Combined Air Operations Center, CENTAF-Forward Public Affairs, "F-15Es, Predator Help Apprehend Insurgents Who Mortared Balad," *Red Tail Flyer,* March 24, 2004.

Cordray Robert C. III, and MAJ (Ret.) Marc J. Romanych, AD, "Out of the Sand: Operational Effects for CJTF-7," *Field Artillery*, January–February 2005, pp. 22–27.

Corum, James S., *The Roots of Blitzkrieg: Hans von Seeckt and German Military Reform,* Lawrence, Kan.: University Press of Kansas, 1992.

Crane, LTC Conrad C. (Ret.), U.S. Army, "Phase IV Operations: Where Wars Are Really Won," *Military Review,* May–June 2005, pp. 27–36.

Crisco, LTC Telford E., Jr., U.S. Army, "The Modular Force: Division Operations," *Military Review,* January–February 2006, pp. 95–100.

Cupp, Staff SGT Jon, U.S. Army, *Deployable Headquarters Units Coming to Fruition,* U.S. Joint Forces Command, undated.

Defense Science Board, "DSB Summer Study on Special Operations and Joint Forces in Support of Countering Terrorism," Final Outbrief, August 16, 2006.

Dempsey, BG Martin E., U.S. Army, "1st Armored Division Commanding General's, briefing from Baghdad," U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), news transcript, December 31, 2003. As of July 2008:
http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=2838

Dervin, Brenda, and Lois Foreman-Wernet, with Eric Lauterbach, *Sense-Making Methodology Reader, Selected Writings of Brenda Dervin,* Cresskill, N.J.: Hampton Press, Inc., 2003.

Dickens, LTC James F., U.S. Army, "Air Component Coordination Element (ACCE) Point Paper," Santa Monica, Calif.: RAND Corporation, unpublished, May 4, 2004.

———, "Service Concept Disconnects and the Future of Air/Ground Integration," Santa Monica, Calif.: RAND Corporation, unpublished, May 14, 2004.

———, *Putting the "O" in Joint DOTMLPF: Organizational Capabilities for Joint Task Force Command and Control,* Carlisle Barracks, Pa.: U.S. Army War College, March 13, 2005.

Doran, ADM Walter F., U.S. Navy, "Pacific Fleet Focuses on War Fighting," *Proceedings*, August 2003, pp. 58–60.

Echevarria, Antulio J. II, *After Clausewitz: German Military Thinkers Before the Great War,* Lawrence, Kan.: University Press of Kansas, 2000.

Edelman, Eric S., Under Secretary of Defense for Policy, "Guidance for Report to the Secretary of Defense on DoD Directive 3000.05 Implementation," Memorandum I-05/003943, March 30, 2006.

England, Gordon, Acting Secretary of Defense, *Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations,* Washington, D.C.: Department of Defense Directive Number 3000.05, November 28, 2005.

Evidence Based Research, Inc., *Network Centric Operations Conceptual Framework,* Version 2.0, prepared for John Garstka, Office of Force Transformation, Vienna, Va., June 2004.

Executive Office of the Headquarters Staff Group, *Army Game Plan,* Office of the Chief of Staff, Army, DACS-ZDV-ESG, 2006. As of July 2008: http://www.army.mil/features/2006ArmyGamePlan/GamePlanOnePgr.pdf

Field, Maj. Walker M., U.S. Marine Corps, "Marine Artillery in the Battle of An Nasiriyah," *Field Artillery,* November–December 2003, pp. 26–30.

Findlay, COL Mike, U.S. Army, LTC Robert Green, U.S. Army, and Maj Eric Braganca, U.S. Air Force, "SOF on the Contemporary Battlefield," *Military Review,* May–June 2003, pp. 8–14.

Fontenot, COL Gregory, U.S. Army (Ret.), LTC F. J. Degen, U.S. Army, and LTC David Tohn, U.S. Army, *On Point: The United States Army in Operation Iraqi Freedom,* Center for Army Lessons Learned, 2004. As of July 5, 2005: http://www.globalsecurity.org/military/library/report/2004/onpoint/index.html

Formica, BG Richard P., and COL Dave Belote, "Integration of Joint Effect in Multi-National Corps–Iraq," briefing at the Joint Fires and Effects Conference, undated.

Frontline Editorial Staff, "3rd Infantry Division Returns to Fort Stewart," *The Frontline,* Vol. 41, No. 2, January 12, 2006.

Futures Development and Integration Center, "Tactics, Techniques, and Procedures for Tactical Operations Involving Sensitive Sites," Version 1.0, Ft.

Leavenworth, Kan.: U.S. Army Combined Arms Center, St 3-90.15,December 2002.

Garamone, Jim, "1st Cavalry Division Takes on Baghdad Responsibility," American Forces Press Service, April 15, 2004. As of July 2008: http://www.defenselink.mil/news/newsarticle.aspx?id=26866

Geraci, Joseph C., "Expert Knowledge in a Joint Task Force Headquarters," *Joint Forces Quarterly,* No. 38, Third Quarter 2005, pp. 53–59.

Geren, Peter, Secretary of the Army, "Address to LandWarNet Conference," Florida, 2007.

Ghosh, Bobby, "The Enemy's New Tools in Iraq," *Time*, June 25, 2007.

Giordono, Joseph, "British General Will Lead Mission in Afghanistan—First Time U.S. Troops Have Followed a Foreign Commander Since WWII," *Mideast Stars and Stripes,* March 11, 2006. As of July 2008: http://www.stripes.com/article.asp?section=104&article=34764&archive=true

Glazier, Jack D., and Ronald R. Powell, *Qualitative Research in Information Management,* Englewood, Colo.: Libraries Unlimited, Inc., 1992.

GlobalSecurity.org, "January 2004 Military News," January 22, 2004. As of July 2008: http://www.globalsecurity.org/military/library/news/2004/01/01-22_index.htm

Gott, Kendall D., ed., *Eyewitness to War,* Volume I, *The U.S. Army in Operation ALFAJR: An Oral History,* Ft. Leavenworth, Kan.: Combat Studies Institute Press, 2006.

Graham, Bradley, "Shortfalls of Special Operations Command Are Cited," *Washington Post,* November 17, 2005, p. 2.

Guitard, Patty, DCGS-A, Army G-2 Information Management Directorate, R&S Division, *Status, Army G2 Information Technology Note to the Field—November/ December 2007.*

Haftendorn, Helga, "Germany's Accession to NATO: 50 Years On," *NATO Update,* May 6, 2005. As of June 11, 2008: http://www.nato.int/docu/update/2005/05-may/e0506a.htm

Harvey, Francis J., Secretary of the Army, and GEN Peter J. Schoomaker, "A Statement on the Posture of the United States Army 2006," presented to the Committees and Subcommittees of the United States Senate and the House of Representatives, 2nd Session, 109th Congress, February 10, 2006.

Headquarters, U.S. Department of the Army, "Five Layer Network Maturation Plan Army Network Strategy Briefing," One on One Network Brief, v2, Washington, D.C., undated.

———, *The Tank and Mechanized Infantry Battalion Task Force,* Field Manual 71-2, Washington, D.C., September 27, 1988.

———, *The Armored and Mechanized Infantry Brigade,* Field Manual 71-3, Washington, D.C., January 8, 1996a.

———, *Battlefield Coordination Detachment (BCD),* Field Manual 100-13, Washington, D.C., September 5, 1996b.

———, *Mission Command: Command and Control of Army Forces,* Field Manual 6-0, Washington, D.C., August 2003.

———, G-3/7 Force Management, "49F Support Brigade Basing and Theater Level CS & CSS Basing, In-Progress Review," briefing, September 30, 2005. Not available to the general public.

———, *Counterinsurgency,* Field Manual 3-24, December 2006. As of January 16, 2009:
http://www.fas.org/irp/doddir/army/fm3-24.pdf

Hersman, Rebecca K. C., *Eliminating Adversary Weapons of Mass Destruction: What's at Stake?* Washington, D.C., and Norfolk, Va.: National Defense University, Center for the Study of Weapons of Mass Destruction, Occasional Paper 1, December 2004. As of July 2008:
http://www.stormingmedia.us/82/8206/A820644.html (subscription required)

Hersman, Rebecca K. C., and Todd M. Koca, "Eliminating Adversary WMD: Lessons for Future Conflicts," *Strategic Forum,* No. 211, October 2004, pp. 1–6. As of July 2008:
http://www.ndu.edu/inss/strforum/SF211/SF211_Final.pdf

Himpelmann, CPT Joseph, U.S. Army, "Catamounts Host Forces Command, Task Force 76 Commanders," press release, Combined Forces Command–Afghanistan Coalition Press Information Center, April 7, 2006.

Holland, Gen Charles R., U.S. Air Force, Commander, U.S. Special Operations Command, statement before the House Armed Service Committee, U.S. House of Representatives, on the state of Special Operations Forces, Washington, D.C., March 12, 2003.

Hollis, Patrecia Slayden, ed., "Victory in Iraq," interview with LTG W. Scott Wallace, Commanding General of V Corps in Iraq During OIF, *Field Artillery,* September–October 2003, pp. 5–9.

———, "Division Operations Across the Spectrum: Combat to SOSO in Iraq," interview with MG Raymond T. Odierno, U.S. Army, Commanding General of the 4th Infantry Division (Mechanized), Ft. Hood, Tex., *Field Artillery,* March–June 2004, pp. 9–12.

———, "Part 1: Joint Effects for the MNC-I in OIF II," interview with BG Richard P. Formica, U.S. Army, Former Commander, Force FA Headquarters (FFA HQ) and Joint Fires and Effects Coordinator, Multinational Corps, Iraq (MNC-I), *Field Artillery,* May–June 2005, pp. 5–9.

HQDA—*See* Headquarters, U.S. Department of the Army.

Hughes, Maj. Roger D., U.S. Marine Corps, "Emergency in Kenya: Kikuyu and the Mau Mau Insurrection," Quantico, Va.: Marine Corps Command and Staff College, April 2, 1984.

Hutcheson, MAJ John, "Balad Predator Strikes Insurgents Placing Roadside Bomb near Balad," *Red Tail Flyer,* March 31, 2004, p. 5.

Information Operations Collections and Analysis Team (CAST), Foreword to Initial Impressions Report No. 05-03, Ft. Leavenworth, Kan.: Center for Army Lessons Learned, May 2005.

Institute for Defense Analysis, "IDA Modularity Study: Working Papers Prepared for Land Forces Division OASD (PA&E)," draft, Alexandria, Va., September 19, 2005.

Iraq Survey Group, "Findings on Iraqi WMD Activities," June 2003–September 2004.

Jacobsen, Mark, "Only by the Sword: British Counter-Insurgency in Iraq, 1920," *Small Wars and Insurgencies,* Vol. 2, No. 2, August 1991, pp. 323–363.

Joint Forces Command, SECDEF Memorandum, Subject "Joint Task Force Headquarters (JTF HQ) Requirements/QDR 2006 Guidance," August 18, 2005.

Joint Task Force Civil Support Public Affairs, *Joint Task Force Civil Support Joins Katrina Relief Effort,* September 1, 2005.

Jones, LTC Mark, U.S. Army, and LTC Wes Rehorn, U.S. Army, "Integrating SOF into Joint Warfighting," *Military Review,* May–June 2003, pp. 3–7.

Josar, David, "New Center Streamlines EUCOM Operations," *Stars and Stripes,* European Edition, January 10, 2004.

Kauchak, Marty, "Winning the War of Ideas," Special Operations Technology Online Archives, Vol. 3, No. 5, August 16, 2005.

Kirkpatrick, Charles E., Corps Historian, "V Corps in the Combat Phase of Operation Iraqi Freedom: Some Notes and a Summary," U.S. Army V Corps, Heidelberg, Germany, March 26, 2004. As of July 2008: http://www.vcorps.army.mil/History/V_Corps_condensed_history_OIF-combat_phase.pdf

———, *Joint Fires as They Were Meant to Be: V Corps and the 4th Air Support Operations Group During Operation Iraqi Freedom,* National Security Affairs

Paper, Arlington, Va.: The Institute of Land Warfare, The Land Warfare Papers, No. 48, October 2004.

Kranepuhl, COL Randolph, Chief of Operations, First U.S. Army, "JTF Katrina—JTF-Katrina Commander's Assessment," briefing, August 31, 2005.

Laird, SGT 1st Class Keith, "2-1 Armored Div. Transfers Authority of Western Baghdad to 2-1 Inf. Div.," Multi-National Corps Iraq, Public Affairs Office, Camp Victory, Press Release No. 20061108-08, November 8, 2006.

Lanza, COL Stephen R., MAJ Robert L. Menti, CPT Luis M. Alvarez, and 1LT Michael R. Dalton, "1st Cav Div Arty as a Maneuver BCT," *Field Artillery,* May–June 2005, pp. 10–16.

Lecakes, LTC George D., XO, Guardian Brigade, "The 20th Support Command (CBRNE)—Worldwide Chemical Conference and Exhibition XXI," briefing, U.S. Forces Command, 2004.

Longoria, COL Michael, ACC/CCJ(JAGO), "Joint Air-Ground Combat," Headquarters, Air Combat Command briefing to the Scientific Advisory Board, February 23–24, 2005.

Lopez, Robert J., and Rich Connell, "A Deadly Day for Charlie Company," *Los Angeles Times,* August 26, 2003. As of November 2003: http://articles.latimes.com/2003/aug/26/world/fg-battle26

"Malayan Emergency," Wikipedia, undated. As of June 2008: http://en.wikipedia.org/wiki/Malayan_Emergency

Manley, Jim, "CJTF Essential Capabilities and Component Capability Offsets," CJTF and Component Essential Capability Analysis, draft briefing, August 2, 2004.

Mattis, LtGen. James N., U.S. Marine Corps, and LtCol. (Ret.) Frank G. Hoffman, U.S. Marine Corps Reserve, "Future Warfare: The Rise of Hybrid Wars," *Proceedings*, November 2005, pp. 18–19.

McFate, Montgomery, "Iraq: The Social Context of IEDs," *Military Review,* May–June 2005, pp. 37–40.

McGrath, John J., *Boots on the Ground: Troop Density in Contingency Operations,* Global War on Terrorism Occasional Paper 16, Ft. Leavenworth, Kan.: Combat Studies Institute Press, 2006.

McKiernan, LTG David D., Commanding General, Third U.S. Army, Commander, U.S. Army Forces Central Command, Coalition Joint Forces, Land Component Command, "Maintaining Momentum in the War on Terrorism," *ARMY*, October 2004, pp. 191–198.

Measuring Stability and Security in Iraq, Report to Congress in accordance with the DoD Appropriations Act 2008, March 2008.

Metz, LTG Thomas F., "Operation Iraqi Freedom II," undated briefing. Not available to the general public.

———, DCG/CoS TRADOC, "Information-Enabled Joint Warfighting and Supporting Capabilities," August 23, 2007.

Miles, Donna, "Joint Force Elements Improve Crisis Response, Combat Ops," American Forces Press Service, March 23 2006a.

———, "Military Providing Full-Scale Response to Hurricane Relief Effort," American Forces Press Service, September 1, 2006b.

Mitchell, LTC Calvin, "DCGS-A, V4—Innovations for the Warfighter," *Army* AL&T, April–June 2007, pp. 32–35.

Mortensen, Daniel R., *A Pattern for Joint Operations: World War II Close Air Support North Africa,* Washington, D.C.: Office of Air Force History and U.S. Army Center of Military History, Historical Analysis Series, No. 93-7, 1987.

Moseley, Lt Gen T. Michael, U.S. Air Force, *Operation Iraqi Freedom—By the Numbers,* U.S. Central Command Air Forces, April 30, 2003.

Multi-National Force–Iraq, "Ironhorse Soldiers Highlighted," November 14, 2006. As of July 2008:
http://www.mnf-iraq.com/index.php?option=com_content&task=view&id=7240&Itemid=21

Multi-National Security Transition Command–Iraq TRAIN. As of February 10, 2009:
http://www.mnstci.iraq.centcom.mil/

NATO—*See* North Atlantic Treaty Organization.

North Atlantic Treaty Organization, *Summit Final Communiqué,* February 20–25, 1952. As of June 2008:
http://www.nato.int/docu/comm/49-95/c520225a.htm

———, North Atlantic Military Committee, *The Most Effective Pattern of NATO Military Strength for the Next Few Years—Report No. 2,* Decision on M.C. 48/1, December 9, 1955. As of June 2008:
http://www.nato.int/docu/stratdoc/eng/a551209a.pdf

Odierno, MG Raymond T., U.S. Army, and LTC Edward J. Erickson, U.S. Army (Ret.), "The Battle of Taji and Battle Command on the Move," *Military Review,* July–August 2003, pp. 2–8.

Odierno, Raymond T., Nichoel E. Brooks, and Francesco P. Mastracchio, "ISR Evolution in the Iraqi Theater," *Joint Force Quarterly,* No. 50, 3rd Quarter 2008, pp. 51–55. As of October 15, 2008
http://www.ndu.edu/inss/Press/jfq_pages/editions/i50/14.pdf

Office of the Secretary of Defense, Program Analysis and Evaluation, *Ground Force Capability Study—Findings,* Washington, D.C., October 20, 2005. Not available to the general public.

Operation Iraqi Freedom Combined Joint Task Force, "CJTF-7 Joint Manning Document," video eleconference, November 5, 2003.

———, "CJTF-7 OIF Force Flow Conference," briefing, Scott Air Force Base, Ill., May 3–14, 2004.

Osborne, Kris, "U.S. Army Sees First UAV Kills," *Defense News,* September 17, 2007, p. 4.

Pagels, Michael, "HURT II (Heterogeneous Unmanned Reconnaissance Team) Development and Evaluation," briefing, Arlington, Va.: Defense Advanced Research Projects Agency, February 2008.

Paparone, COL Christopher R., U.S. Army, and James A. Crupi, "What Is Joint Interdependence, Anyway?" *Military Review,* July–August 2004, pp. 39–41.

Peterson, Lt Col Bill, Chief, Experiment and Wargame Division, U.S. Air Force, "Air Component Coordination Element (ACCE)," briefing, Maxwell Air Force Base, Ala.: Air Force Doctrine Center, May 2, 2006.

Price, Johann, "Operation Enduring Freedom: Commands and HQS June 1, 2002," V.1.1, June 23, 2002.

Pryor, SGT Mike, "Human Terrain Team Helps Soldiers in Iraq Understand Cultural Landscape," Army News Service, December 11, 2007.

Red Team, First Cavalry Division, "The '3 Muhalla War': 5 Lines of Operation in 5 BCT," briefing, undated. Not available to the general public.

Reis, CDR Ronald, U.S. Navy, and LCDR Glenn F. Robins, U.S. Navy, "Integrating Carrier-Based Electronic Attack into Conventional Army Doctrine," *Military Review,* May–June 2003, pp. 21–25.

Ross, Blair A., Jr., "The U.S. Joint Task Force Experience in Liberia," *Military Review,* May 1, 2005, pp. 60–67.

Rumsfeld, Donald, U.S. Secretary of Defense, *Policy Implementation to Improve Formation and Sustainment of Joint Task Force (JTF) Headquarters,* Memorandum to the Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Commanders of the Combatant Commands, Assistant Secretaries of Defense, Directors of Defense Agencies, and Chief, National Guard Bureau, Washington, D.C., February 4, 2005.

———, "SECDEF Memo for JTF's," Washington, D.C., February 4, 2005.

Schonlau, Matthias, Ronald D. Fricker, and Marc N. Elliott, *Conducting Research Surveys via E-Mail and the Web,* Santa Monica, Calif.: RAND Corporation,

MR-1480-RC, 2002. As of January 19, 2009:
http://www.rand.org/pubs/monograph_reports/MR1480/

Schreckengost, CPT Gary J., U.S. Army, and CPT Gary A. Smith, PAARNG, "IO in SOSO at the Tactical Level: Converting Brigade IO Objectives into Battalion IO Tasks," *Field Artillery,* July–August 2004, pp. 11–15.

Schreiber, CDR Steven P., U.S. Navy, LTC Greg E. Metzgar, U.S. Army, and Maj Stephen R. Mezhir, U.S. Air Force, "Behind Friendly Lines: Enforcing the Need for a Joint SOF Staff Officer," *Military Review,* May–June 2004, pp. 2–8.

Science Applications International Corporation, *Managing and Maintaining Linguistic Resources: Defense Language Transformation Task 4,* Executive Summary, undated.

Scott, COL Randle, U.S. Army, "Elimination Operations," draft briefing, U.S. Strategic Command, U.S. Defense Threat Reduction Agency, undated. Not available to the general public.

Shachtman, Noah, "Drone, Copter Team Kills 2,400 Bombers in Iraq," *Wired News,* January 21, 2008. As of March 8, 2009:
http://blog.wired.com/defense/2008/01/drone-copter-te.html

Singer, Jeremy, "Bandwidth Breakthrough," *Air Force Magazine Online,* Vol. 90, No. 3, March 2007.

Spartan Sentinel, Vol. 2, No. 2, November 14, 2006.

Special Operations Command Joint Forces Command, *Joint Special Operations Insights No. 6*, April 2004.

Spitz, Lt Col Mike, ACC/XPPC, "Air Force Support to Army Transformation," Headquarters, Air Combat Command, briefing, March 11, 2005. Not available to the general public.

Stata Corporation, Stata Statistical Software: Release 7.0, College Station, Tex., 2001.

Stevens, CPT Roger M., and MAJ Kyle M. Marsh, "3/2 SBCT and the Countermortar Fight in Mosul," *Field Artillery,* January–February 2005, pp. 36–39.

Sweet, LTC Jonathan E., U.S. Army, "741st Military Intelligence Battalion Command Philosophy," July 10, 2007.

Tait, COL William, U.S. Army, III Corps G-2, "MNC-I Intelligence Observations," briefing, 2007.

Talbot, David, "How Tech Failed in Iraq," *Technology Review,* November 2004, pp. 36–44.

Task Force Baghdad/4ID, "3ID Passes Responsibility to 4ID During 'Transfer of Authority' Ceremony Saturday," Media Advisory Release No. 20060106-01, January 6, 2006.

Tiron, Roxana, "Special Operators Must Change to Win War," *National Defense,* April 2004. As of July 2008: http://www.nationaldefensemagazine.org/archive/2004/April/Pages/Special_Operators3608.aspx

Tyson, Ann Scott, "No Drop in Iraq Violence Seen Since Troop Buildup," *Washington Post,* June 14, 2007.

Tyson, Ann Scott, and Glenn Kessler, "CENTCOM Pick Warns of Iran Influence in Gulf Region," *Washington Post,* January 31, 2007, p. A11.

U.S. Air Force, *Operations and Organization,* Air Force Doctrine Document 2, Washington, D.C., April 17, 2006.

U.S. Air Force Doctrine Center, *Air Component Coordination Element Handbook,* Air Force Doctrine Center Handbook 10-03, Headquarters, U.S. Air Force Doctrine Center/DR, September 6, 2005.

U.S. Air Force Scientific Advisory Board, "Report of the Ad Hoc Committee on Options for Theater Air Defense," SAB-TR-93-01, Washington, D.C., November 2006.

U.S. Army, *Serving a Nation at War: A Campaign Quality Army with Joint and Expeditionary Capabilities,* Version 9.9, April 30, 2004. As of July 2008: http://www.army.mil/howwewillfight/

———, "Capabilities Overview," Ft. Lewis, Wash.: 3/2 SBCT Arrowhead Brigade, February 2006a.

———, Annex D, *Army Modernization Plan 2006,* Headquarters, U.S. Army, March 24, 2006b.

———, "Big Red One and Ft. Riley Community Update," Vol. 1, No. 2, Ft. Riley, Tex., March 2007.

U.S. Army Forces Command, "Requirements-Based Construct," briefing, Ft. McPherson, Atlanta, Ga., May 13, 2005.

———, Army Review Council, "ACP Decision Point 45 ARFORGEN Implementation Strategy," Ft. McPherson, Atlanta, Ga., June 23, 2005.

U.S. Army, Headquarters, 1st Infantry Division, "Breaking the Cycle of Violence" and "Iraqi Armed Services Recruiting Center Opens," press releases, Tikrit, Iraq (Forward Operating Base Danger), January 2, 2005.

U.S. Army Training and Doctrine Command, "LandWarNet final briefing to Defense Advanced Research Projects Agency FCS Senior Advisory Group," April 2006a.

———, "The United States Army Concept for Operational Maneuver," TRADOC Pamphlet 525-3-1, Version 1.0, October 2, 2006b.

———, "The United States Army's Operating Concept for Tactical Maneuver," TRADOC Pamphlet 525-3-2, Version 1.0, October 2, 2006c.

———, "The United States Army Functional Concept for Strike 2015–2024," TRADOC Pamphlet 525-3-4, April 30, 2007.

U.S. Army, 75th Field Artillery Brigade, "75th XTF Lessons Learned, Diamond Team," briefing, undated.

U.S. Department of the Army, "3-Star Uex Design Development IPR," briefing, July 25, 2005.

———, "AFORGEN and Contingency Planning: Synchronizing the Army's Force Provider Methodology and Joint Operations Planning," briefing No. DA G35-SSW August 25, 2005. Not available to the general public.

———, "Adapting the MACOM Structure/Army Campaign Plan Decision Point #58/Phase I: Army MACOM Structure/Phase II: Theater Support Structure," unpublished briefing, October 20, 2005. Not available to the general public.

———, "Phase I: Lines of Authority—COAs for Army Commands, ASCCs, and DRUs," unpublished briefing, October 28, 2005.

U.S. Department of the Army, Procurement Programs, *Committee Staff Procurement Backup Book Fiscal Year (FY) 2008/2009 Budget Estimate,* Communications and Electronics Budget Activity 2 Appropriation, Washington, D.C., 2007.

U.S. Department of Defense, *Final Report of the Independent Panel to Review DoD Detention Operations,* Washington, D.C., August 2004. As of July 2008: http://www.defenselink.mil/news/Aug2004/d20040824finalreport.pdf

———, "Department of Defense Capabilities for Stability Operations," Department of Defense Directive Number 3000.ccE, draft, Washington, D.C., February 28, 2005.

———, *The National Defense Strategy of the United States of America,* Washington, D.C., March 2005. As of March 16, 2009: http://www.comw.org/qdr/fulltext/0503nds.pdf

———, "Net-Centric Environment Joint Functional Concept," Version 1.0, Washington, D.C., April 7, 2005.

———, *Strategy for Homeland Defense and Civil Support,* Washington D.C., June 2005. As of July 2008: http://www.defenselink.mil/news/Jun2005/d20050630homeland.pdf

———, *Quadrennial Defense Review Report,* Washington, D.C., February 6, 2006. As of June 2008:
http://www.defenselink.mil/qdr/

———, *Measuring Stability and Security in Iraq,* Quarterly Reports to Congress, Washington, D.C., March 2008. As of July 2008:
http://www.defenselink.mil/home/features/Iraq_Reports/

U.S. Joint Chiefs of Staff, *The National Military Strategic Plan for the War on Terrorism (NMSP-WOT),* Washington, D.C., March 29, 2005.

U.S. Joint Forces Command, "Forming and Sustaining Joint Task Force Headquarters: A Discussion," briefing, Norfolk, Va., November 2, 2004.

———, Strategic Planning Guidance 2006–2011, Directed Study Task 04, *Expanding the Joint C2 Capability of Service Operational Headquarters,* Final Report, Version 17, Norfolk, Va., February 17, 2005.

———, *United States Joint Forces Command Glossary,* October 28, 2005.

U.S. Marine Corps, 1st Marine Division, "Operation Iraqi Freedom (OIF): Lessons Learned," May 2003.

Urrutia, Alex, U.S. Joint Forces Command/Director JBMC2, "Joint Command and Control (JC2) Capability (QDR status)," JBMC2 BOD briefing, U.S. Joint Forces Command, Norfolk, Va., December 15, 2005.

Van Pelt, COL Raymond T., and Jim Currie, PFA, *JTF—WMD Elimination: An Operational Architecture for Future Contingencies,* Ft. McNair, Washington, D.C.: The Industrial College of the Armed Forces, National Defense University, April 28, 2004.

Vane, LTG Michael A., U.S. Army, Director, Army Capabilities Integration Center, "The United States Army's Concept of Operations (CONOPS), LandWarNet 2015," Version 2.0, September 5, 2007.

Vines LTG John R., U.S. Army, XVIII Airborne Corps/Multi-National Corps–Iraq, *Initial Impressions Report,* 06-27, Ft. Leavenworth, Kan.: Center for Army Lessons Learned, May 2006.

———, "The XVIII Airborne Corps on the Ground in Iraq," *Military Review,* September–October 2006, pp. 38–46.

von Mellenthin, Friedrick Wilhelm, *Panzer Battles: A Study of the Employment of Armor in the Second World War,* New York: Ballantine Books, 1971.

Wallace, LTG William, Commander, V Corps, "V CORPS: Bottom Line Up Front—The Road to 'Victory' in Operation Iraqi Freedom," unpublished briefing, October 10, 2003.

———, U.S. Army, "Network-Enabled Battle Command," *Military Review,* May–June 2005, pp. 2–5.

———, Commanding General, Training and Doctrine Command, "Leading Change to Deliver Joint Warfighting Capabilities," August 24, 2006.

Waring, COL James M., LTC Carl L. Giles, AV, and Chief Warrant Officer Three John A. Robinson, "The 19th BCD in Counterinsurgency Operations," *Field Artillery,* July–August 2005, pp. 16–19. As of July 2008: http://sill-www.army.mil/FAMAG/2005/JUL_AUG_2005/PAGES16_19.pdf

Wendel, BG Kevin R., "20th Support Command (CBRNE) Capabilities Brief and Way Ahead," U.S. Army Forces Command briefing, May 1, 2006.

White, John P., Deputy Secretary of Defense, *Department of Defense Counterproliferation (CP) Implemention,* Department of Defense Directive Number 2060-2, Washington, D.C., July 9, 1996.

Whitten, Lt Col Duke, "JTF/JFC HQ Training and Certification Criteria and Standards," Headquarters, U.S. European Command, briefing, August 9, 2005.

Wilsoncraft, Spc. Emily J., 3rd Infantry Division, "U.S. 3rd Infantry Division Assumes Task Force Baghdad Mission," Third Army U.S. Army Central Coalition Forces Land Component Command, news story, March 1, 2005.

"Winning the War of Ideas," *Special Operations Technology,* online ed., Vol. 3, No. 5, August 16, 2005.

Wolf, MAJ John, *TF ODIN: Airborne RSTA Army G2 Information Technology Note to the Field,* November–December 2007.

Wood, MG John R., "Joint Command and Control Integrating Concept Way Ahead Brief," briefing, JFCOM/J9, August 16, 2006.

Worley, D. Robert, "Joint Task Forces: Options to Train, Organize, and Equip," *National Security Studies Quarterly,* Vol. V, No. 1, Winter 1999, reprint, pp. 31–48.

Zimmerman, COL Douglas K., U.S. Army, "Understanding the Standing Joint Force Headquarters," *Military Review,* July–August 2004, pp. 28–32.